DESHPANDE & ASSOCIATES

Chartered Accountants

Flat no. 4, Manisha App, Near Udyog Bhavan
Saraswatinagar, Sangli.

Email: cadeshpandeassociates2006@gmail.com

Mobile no.: 9423829680

INFORMATION SYSTEM AUDIT

&

VAPT

DESHPANDE & ASSOCIATES
CHARTERED ACCOUNTANTS
FLAT NO 4, MANISHA APARTMENT, SARASWATINAGAR, NEAR UDYOG BHAVAN,
SANGLI-416416
M 9423829680 O. 0233-2672888
EMAIL: cadeshpandeassociates2006@gmail.com

D.Y. PATIL EDUCATION SOCIETY KOLHAPUR
INFORMATION SYSTEM AUDIT REPORT

AUDIT CONDUCTED BY
M/S DESHPANDE & ASSCOCIATES
FCA DISA CISA

For Deshpande & Associates

Chartered Accountant

DESHPANDE & ASSOCIATES * Chartered Accountants * FRN 136235W

Dheeraj Deshpande

M. No. 119824

B.com, FCA, DISA, CISA

DESHPANDE & ASSOCIATES
CHARTERED ACCOUNTANTS
FLAT NO 4, MANISHA APARTMENT, SARASWATINAGAR, NEAR UDYOG BHAVAN,
SANGLI-416416
M 9423829680 O. 0233-2672888
EMAIL: cadeshpandeassociates2006@gmail.com

DESHPANDE & ASSOCIATES * Chartered Accountants * FRN 136235W

Audit start date: 20/06/2022

Audit end date: 12/07/2022

Audit conducted by: Deshpande & Associates (Chartered Accountants)

Dheeraj Deshpande (B.com, FCA,DISA,CISA)

Nitin Kedar (B Com)

Omkar Dhumal (B.Com)

Audit representatives from Organization :

Shri Ramesh Randive(IT In charge)

Shri Prasanna Pandit (IT Officer)

DESHPANDE & ASSOCIATES
CHARTERED ACCOUNTANTS
FLAT NO 4, MANISHA APARTMENT, SARASWATINAGAR, NEAR UDYOG BHAVAN,
SANGLI-416416
M 9423829680 O. 0233-2672888
EMAIL: cadeshpandeassociates2006@gmail.com

DESHPANDE & ASSOCIATES FRN 136235W Chartered Accountants

Executive Summary :

We have conducted computer environment and procedural audit of D.Y. PATIL EDUCATION SOCIETY KOLHAPUR

IS audit objectives:-

The objective of IS audit is to ensure integrity, confidentiality & availability of data & to safeguard the assets of the Organization by conducting review of application software, DBMS, hardware & networking components & IT general controls & environmental controls.

IS audit scope:-

1. Application software review
2. IT general controls review
3. IT environmental controls review
4. Hardware & networking components review
5. Data center inspection
6. Application Modules review
7. Review of CBS agreement, other agreements , insurance and policies.

DESHPANDE & ASSOCIATES
CHARTERED ACCOUNTANTS
FLAT NO 4, MANISHA APARTMENT, SARASWATINAGAR, NEAR UDYOG BHAVAN,
SANGLI-416416
M 9423829680 O. 0233-2672888
EMAIL: cadeshpandeassociates2006@gmail.com

DESHPANDE & ASSOCIATES FRN 136235W Chartered Accountants

Synopsis of CBS Application and Database:

- Application software developed by: Manorama Infosolutions Pvt. ltd.
- Application software version : Lifeline Corporate Suite
- Database server version : SQL 2017
- Operating system : Windows Sever 2016 Standard

DESHPANDE & ASSOCIATES
CHARTERED ACCOUNTANTS
FLAT NO 4, MANISHA APARTMENT, SARASWATINAGAR, NEAR UDYOG BHAVAN, SANGLI-416416
M 9423829680 O. 0233-2672888
EMAIL: cadeshpandeassociates2006@gmail.com

INDEX

DESHPANDE & ASSOCIATES
CHARTERED ACCOUNTANTS
FLAT NO 4, MANISHA APARTMENT, SARASWATINAGAR, NEAR UDYOG BHAVAN,
SANGLI-416416
M 9423829680 O. 0233-2672888
EMAIL: cadeshpandeassociates2006@gmail.com

DESHPANDE & ASSOCIATES * Chartered Accountants * FRN 136235W

Criteria for Risk Grading

(*) Risk Analysis Grading:

- **H (High Risk) :**
  Issue poses High Risk and warrants immediate PREVENTIVE INTERNAL CONTROLS by the management. Immediate management attention is required.

- **M (Medium Risk) :**
  Issue poses Medium Risk. Management is expected to incorporate sufficient PREVENTIVE OR DETECTIVE INTERNAL CONTROLS IN THE PROCESS.

- **L (Low Risk) :**
  Issue poses Low Risk. Process oriented observation but still cognizance need to be taken by the management to improve the process and strengthen the OVERALL INTERNAL CONTROL ENVIRONMENT

DESHPANDE & ASSOCIATES
CHARTERED ACCOUNTANTS
FLAT NO 4, MANISHA APARTMENT, SARASWATINAGAR, NEAR UDYOG BHAVAN,
SANGLI-416416
M 9423829680 O. 0233-2672888
EMAIL: cadeshpandeassociates2006@gmail.com

Information System Audit Report

Areas of Audit	Findings & Observations	Auditor's Remarks
1. Access controls • The system allows access to only authorized users. • System requests for identification and new password before login into the system. • System has password mechanisms, which restrict the access to authenticate users.	1. Currently user wise access rights are created in the system. 2. Authority – Responsibility Chart is not created in the organization.	1. Authority responsibility chart should be prepared.
2. Encryption and Data Confidentiality □ The system uses SSL or similar session confidentiality protection mechanisms □ The system uses a secure storage mechanism for storing of usernames and passwords. • The system adequately protects the confidentiality of the user's trade data. • The system used security encryption to ensure confidentiality off sessions initiated. • Session initiation and termination events are logged	1. Encryption is adopted for Stored Data. 2. Event logs are logged but not monitored. 4. Confidentiality regarding off sessions not ensured. 5. Protection of user's trade data is not adequate.	1. Possibility of adopting an encryption mechanism should be explored for data to be kept on Database server 2. Policy should be prepared for Data Confidentiality 3. Data analysis should be done for a) Publicly available data b) Highly sensitive data c) Data available subject to authorization 4. Event log monitoring task should be assigned to evaluate performance of employees.

DESHPANDE & ASSOCIATES
CHARTERED ACCOUNTANTS
FLAT NO 4, MANISHA APARTMENT, SARASWATINAGAR, NEAR UDYOG BHAVAN,
SANGLI-416416
M 9423829680 O. 0233-2672888
EMAIL: cadeshpandeassociates2006@gmail.com

<table>
<tr>
<td>and audited.
• The system allows only authorized and validated users to establish</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3.Backup procedure for
Application level
☐ Database
☐ Audit Trails
• Reports
At the user level
☐ Logs
☐ History
☐ Reports
• Audit Trails
<table>
<tr><th></th><th>Yes</th><th>No</th></tr>
<tr><td>Are backup procedures documented?</td><td>Yes</td><td></td></tr>
<tr><td>Are backup logs maintained?</td><td>Yes</td><td></td></tr>
<tr><td>Have the backups been verified and tested?</td><td></td><td>No</td></tr>
<tr><td>Are the backup media stored safely in line with the risk involved?</td><td>Yes</td><td></td></tr>
<tr><td>Are there any recovery procedures and have the same been tested?</td><td>Yes</td><td>Not tested</td></tr>
</table>
</td>
<td>1. Documented Backup procedure is there.
2. Backup logs are not maintained
3. Back up Register is not maintained.
4. Backups are not checked for restorations.
5. No formal policy and training for restoration.
6. Total Data Size : 2 To 3 Gb.</td>
<td>1. There should be a separate Back up documentation & restoration procedure
2. Separate stand by server is there in the data center but back up is not restored on it regularly. See Data Center remarks for further explanation
3. Back up should be taken on Pen drive as well as DVD or CD. I.e. Different medias should be used and both the two should be stored at different locations.
4. Currently no formal policy for restoration of back ups.
Restoration policy should be prepared and back ups should be timely restored At Head Office level.
5. Back up is taken on external hard disk but this external hard disk is not stored off site.
6. Back up time is taken approx. 2 hours. It should be reduced to reasonable</td>
</tr>
</table>

DESHPANDE & ASSOCIATES
CHARTERED ACCOUNTANTS
FLAT NO 4, MANISHA APARTMENT, SARASWATINAGAR, NEAR UDYOG BHAVAN,
SANGLI-416416
M 9423829680 O. 0233-2672888
EMAIL: cadeshpandeassociates2006@gmail.com

Are back up of Registries maintained? — No		level.
4.Network Related: • Verify location(s) of nodes in the network • Verify number of nodes in diagram with actual	Connected through Broad band connectivity is used for Server. Data bandwidth : Primary : 1 Gbps Secondary : Airtel 10Mbps.	
5.Physical Security: For Hardware For Software For systems Control on admission of personnel location Audit trails of all the entries-exits at Location	1. PCs at user level do not have CD and DVD drives and Pen drive disabled.	1. Server should not be kept in open environment. It should be kept in Server Room 3. Pen drives DVD/CD drives should be disabled for systems where there is no need. 4. Strict control should be exercised on external devices like CDs, DVDs and Pen drives also.
6.Password Policies Does installed application system's use passwords for authentication? — Yes Is password policy / standard is documented. — Yes System mandated changing of password when the user logs in for the first time — No Automatic disablement of the user on entering erroneous password on three consecutive occasions — No		1. Passwords should be changed for every 14 days. 2. After every 14 days, system should prompt for changing password. 3.System should not accept same password again 4. For Admin passwords, there should be a "Sealed Envelope" procedure implemented. 5. After every three unsuccessful login attempts,

DESHPANDE & ASSOCIATES
CHARTERED ACCOUNTANTS
FLAT NO 4, MANISHA APARTMENT, SARASWATINAGAR, NEAR UDYOG BHAVAN,
SANGLI-416416
M 9423829680 O. 0233-2672888
EMAIL: cadeshpandeassociates2006@gmail.com

Automatic expiry of password on expiry of 14 calendar days.		No		system should automatically block the respective login id of the user. A log of such transaction should be generated and monitored.
System controls to ensure that the password is alphanumeric (preferably with one special character), instead of just being alphabets or just numerical.		No		
System controls to ensure that the changed password cannot be the same as of the last 10 Passwords		No		
System controls to ensure that the Login id of the user and password should not be the same.		No		
System controls to ensure that the Password should be of minimum six characters and not more than twelve characters.	Yes			
System controls to ensure that the Password is encrypted at members end so that employees of the member cannot view the same at any point of time.		No		
All successful and failed login attempts should be logged with details like User ID, MAC address and other data to enable traceability		No		

7.Policies or Procedures regarding Business Continuity/Disaster Recovery:

	Yes	No
Any documentation on Business Continuity / Disaster Recovery / Incident Response		**No**
BCP / DRP plan exist		**No**
BCP/DRP plan it been tested (If available)		**No**
Incident response procedures available		**No**
Risk assessments procedures available		**No**
Call List for emergencies maintained		**No**
Organization is having DR site		**No**

1.Written and documented DRP/ BCP (Disaster Recovery / Business Continuity Plan) should be prepared.
2. Disaster Recovery Drills should be conducted at least twice a year.
3. Call list for emergency should be prepared and kept on the desk of Manager or Authorized person.
4.Organization is not having

DESHPANDE & ASSOCIATES
CHARTERED ACCOUNTANTS
FLAT NO 4, MANISHA APARTMENT, SARASWATINAGAR, NEAR UDYOG BHAVAN,
SANGLI-416416
M 9423829680 O. 0233-2672888
EMAIL: cadeshpandeassociates2006@gmail.com

<table>
<tr>
<td></td>
<td>Disaster Recovery Site. It Organization should be prepared and configured as soon as possible.
5. Organization is advised to establish DR site in order to follow Disaster Recovery and Business Continuity plan operations.</td>
</tr>
<tr>
<td>8.Network / Communication Link Backup
<table>
<tr><th></th><th>Yes</th><th>No</th></tr>
<tr><td>Backup network link is available in case of failure of the primary link</td><td></td><td>No</td></tr>
<tr><td>Backup network link is available in case of failure of the primary link connecting through the Application</td><td></td><td>No</td></tr>
</table>
</td>
<td>At present every machines are having internet facility. Down time standards should be set and the down time should be kept below those standards</td>
</tr>
<tr>
<td>9.Approvals, Undertaking, Agreements, Policies, Licenses :
<table>
<tr><th></th><th>Yes</th><th>No</th></tr>
<tr><td>Undertaking provided regarding the Application and Database system as per relevant Minutes of Meeting</td><td></td><td>No</td></tr>
<tr><td>Application of approval for Internet Users</td><td></td><td>No</td></tr>
<tr><td>Whether the Insurance policy of the Member covers the additional risk of usage of Application, data, hardware and networking components.</td><td></td><td>No</td></tr>
<tr><td>Whether Software Licensing agreement properly and duly entered and Annual Maintenance Contract updated with software vendor.</td><td>Yes</td><td></td></tr>
</table>
</td>
<td>1. Internet configuration should be made for site restrictions, and regarding agreements and policies should be prepared.
2. Insurance policy with adequate coverage should be taken for all Hardware, Software and Networking devices.
3. Hardware & software vendor A.M.C. (Annual Maintenance Contract) should clearly specify clauses regarding free service and chargeable service.
4. User wise requirement analysis of the licensing should be done regarding Database licenses and Server licenses and</td>
</tr>
</table>

DESHPANDE & ASSOCIATES
CHARTERED ACCOUNTANTS
FLAT NO 4, MANISHA APARTMENT, SARASWATINAGAR, NEAR UDYOG BHAVAN,
SANGLI-416416
M 9423829680 O. 0233-2672888
EMAIL: cadeshpandeassociates2006@gmail.com

<table>
<tr>
<td></td>
<td>it should be ensured that Organization should adopt licensing the users strictly as per requirement so that legal compliance be done strictly.</td>
</tr>
<tr>
<td>10.System Failure Backup
<table>
<tr><th></th><th>Yes</th><th>No</th></tr>
<tr><td>Backups for the critical system components</td><td></td><td></td></tr>
<tr><td>Database Server (See Comment)</td><td>Yes</td><td></td></tr>
<tr><td>Network Switch / Router</td><td></td><td>No</td></tr>
<tr><td>Infrastructure breakdown backup</td><td></td><td></td></tr>
<tr><td>Electricity</td><td>Yes</td><td></td></tr>
<tr><td></td><td></td><td></td></tr>
<tr><td>Air Conditioning</td><td>Yes</td><td></td></tr>
<tr><td>Alternate physical location of employees been made in case of non availability of the primary site</td><td></td><td>No</td></tr>
<tr><td>Provisions for Books and records backup and recovery (hard copy and electronic).</td><td></td><td>No</td></tr>
<tr><td>Mission-critical systems been identified and provision for backup for such systems been made</td><td></td><td>No</td></tr>
</table>
</td>
<td>Separate database server should be kept.
If possible and feasible, Critical systems should be Replicated at a distant site and alternative arrangement for operations for employees should be done in case of any disaster or natural calamity.
It is advised to purchase stand by switch and stand by Application Server.</td>
</tr>
<tr>
<td>11. Day's Activities:
<table>
<tr><th></th><th>Yes</th><th>No</th></tr>
<tr><td>Provision for Begin of day activity</td><td>Yes</td><td></td></tr>
<tr><td>Audit Trails</td><td></td><td>No</td></tr>
<tr><td>Access Logs</td><td></td><td>No</td></tr>
<tr><td>Transaction Logs</td><td>Yes</td><td></td></tr>
</table>
</td>
<td>1. Audit Trails and logs are not getting monitored.
2. It was observed that proper checks are not incorporated in system for conducting EOD process. System should automatically prompt at a certain time for conducting EOD.</td>
</tr>
</table>

DESHPANDE & ASSOCIATES
CHARTERED ACCOUNTANTS
FLAT NO 4, MANISHA APARTMENT, SARASWATINAGAR, NEAR UDYOG BHAVAN,
SANGLI-416416
M 9423829680 O. 0233-2672888
EMAIL: cadeshpandeassociates2006@gmail.com

Backup Logs		No	3. Activity log monitoring system should be incorporated. 4. Time wise BOD & EOD reports should be generated by the system and H.O. Managers should review the same periodically.
Alert Logs		No	
Activity Logs		No	
Provision for End of day activity	Yes		
System for log monitoring, escalation & corrective measures taken, if any.		No	

12. Details of the various response procedures available:

	Yes	No
Access Control failure		No
Day Begin failure		No
Day End failure		No
Other system Processes failure		No

1. There should be a well documented procedure specifying Do's and Don'ts for critical Process Failures. User Manual is kept.
2. Staff should be aware about escalation policies for any system or process failures.

13.Other Areas :

	Yes	No
Firewall implemented	Yes	
Malicious code protection system implemented		No
Instances of infection		No

1. Firewall configuration training should be imparted to the staff.
2. Anti-virus should be installed at all machines. It should be auto scheduled for real time scanning

14. APPLICATION CONTROL REVIEW

1. Server Warranty :

DESHPANDE & ASSOCIATES
CHARTERED ACCOUNTANTS
FLAT NO 4, MANISHA APARTMENT, SARASWATINAGAR, NEAR UDYOG BHAVAN,
SANGLI-416416
M 9423829680 O. 0233-2672888
EMAIL: cadeshpandeassociates2006@gmail.com

It is observed that data center server are out of warranty. It is highly recommended to either purchase new data center servers for both application and database servers. Else extension should be taken for server warranty.

2. We have checked following modules in the CBS application :

1. Registration
2. Billing
3. Medical Record Room (MRD)
4. Enterprise Configuration
5. Inventory
6. Operation Theatre
7. MIS Reports
8. Audit

Following are some of the important observations regarding CBS modules :

3. Registration:

Observation :

We have observed that Aadhar number and date of birth is not fed in the system.

It is observed that KYC is not scanned in the system.

Customer ID parameters are not set in the system.

Recommendation:

It is suggested to the organization that all patient's aadhar number should be mandatorily updated in the system.

It is recommended that KYC should be scanned in the system.

It is recommended to the society that Customer ID parameters should be set in the system.

4. Billing :

Observation :

Currently it is observed that cash Denomination is not fed in the system

Batch wise & user wise Cash should be tallied. It should be tallied twice in a day from the system.

Discount option should have proper authorization.

DESHPANDE & ASSOCIATES
CHARTERED ACCOUNTANTS
FLAT NO 4, MANISHA APARTMENT, SARASWATINAGAR, NEAR UDYOG BHAVAN,
SANGLI-416416
M 9423829680 O. 0233-2672888
EMAIL: cadeshpandeassociates2006@gmail.com

Recommendation:

Denomination should be fed in the system and report should be made available in the system.

Batch wise user wise Cash should be tallied. It should be tallied twice in a day from the system.

Cash reconciliation should be done daily in the system. Cash handover procedure to the accounts department should be compulsorily set from the system so that cash balance at the counter and at the accounts department should be strictly as per CBS system balance.

5. Medical Record Room (MRD)

MRD policy should be created for keeping record retention. For e.g. how many years data should be stored on the live database let's say 5 years or 8 years etc. The data beyond those years should be backed up and stored on a different server so that the server space on the live database server can be freed.

6. Enterprise Configuration:

No observations in this module. This module is used for the IT department mainly for parameters and other configuration.

7. Inventory

Observation :

Currently it is observed that stock item requested and issued stock and remaining stock calculation is not properly done from the system.

Currently it is observed that all machines purchase date are wrongly fed in the system it should be rectified.

It is suggested that the balance of inventory module should be tallied as per the accounting software of the society from time to time.

8. Registers :

We recommend following registers are required to be maintained:

Backup Register,

Vendor Register,

DESHPANDE & ASSOCIATES
CHARTERED ACCOUNTANTS
FLAT NO 4, MANISHA APARTMENT, SARASWATINAGAR, NEAR UDYOG BHAVAN,
SANGLI-416416
M 9423829680 O. 0233-2672888
EMAIL: cadeshpandeassociates2006@gmail.com

Change Management register,
Inventory register

9. Change management Policy :

All types of changes regarding CBS should be documented and before change intimation should be given from CBS vendor.
Society is suggested that record of the changes in CBS software should be maintained.
Detailed note of patch and change should be obtained from the vendor.
The change should be first tested on test server and then only migrated to the live server.
Software version management program should be taken from the vendor.

10. Accounting Module:

Currently it is observed that accounting module is not active in the system. Currently Society is doing accounting from tally. It is highly recommended that accounting should be done through the CBS software only or interface provided this software to tally.

Accounting module should be active from the system and showing all expenditure and income should be accounts.

11. Payroll Module:

Currently it is observed that payroll module is not active on System. Therefore employee leave recorded, incentive, promotion and bonus all this detail are out of the system.

12. SMS Facility:

We have suggested to society SMS Facility should be provided to patient.

13. Following Modules should be implemented in CBS.

Currently it is observed that stationery, Dead-stock and Deprecation, MIS and audit Module are not active in the system.

14. Charges Master :

DESHPANDE & ASSOCIATES
CHARTERED ACCOUNTANTS
FLAT NO 4, MANISHA APARTMENT, SARASWATINAGAR, NEAR UDYOG BHAVAN,
SANGLI-416416
M 9423829680 O. 0233-2672888
EMAIL: cadeshpandeassociates2006@gmail.com

All Charges should be auto generated in the system.

15. Mail Domain :

It currently observed that Society not having separate Email Domain. Society is suggested to purchase separate email domain for suspicious Email.

16. Policy Related Observation :

Following policies should be adopted:

1. Cyber security Policy
2. Network policy
3. Password Policy
4. Internet Policy
5. Database backup policy
6. Database Restoration policy
7. Cyber-attack prevention and Incident Response Policy

17. Insurance :

It is suggested to the organization that Data Center hardware insurance be taken.

It is suggested to the organization that Cyber insurance cover with adequate value should be taken.

18. IT Staff :

It is suggested to the organization that at least one or two IT staff should be hired for server log monitoring, firewall monitoring and data center maintenance and database activities and also for business development related IT issues.

19. IT Policy Points:

Roles and responsibilities should be mentioned in policy.

Password frequency should be mentioned in policy.

Incident response management clause should be inserted in policy.

20. Changes in Application :

Currently it is observed that changes are possible from system it should be restricted and only authorized person can be change.

DESHPANDE & ASSOCIATES
CHARTERED ACCOUNTANTS
FLAT NO 4, MANISHA APARTMENT, SARASWATINAGAR, NEAR UDYOG BHAVAN,
SANGLI-416416
M 9423829680 O. 0233-2672888
EMAIL: cadeshpandeassociates2006@gmail.com

21. Users

It is suggested to the organization user review should be conducted and unused users should be disabled.

We have suggested to society user maker and check should be created.

We observed that Single person having multiple User ID's.

One person should be assigned with only one user id.

22. Scheme Details of Governemnt schemes :

Currently it is observed that Scheme details are not fed in the system. e.g. Sanction Amount , Approval details.

This is suggested in Registration module.

23. Technology development fund

It is suggested to the society technology development fund should be created every year out of profit for atleast 2 to 5 %.

15. NETWORK RELATED OBSERVATIONS :

I. It is suggested to the organization IP segmentation should be implemented.
II. Currently it is observed that full internet access is given to all users it is recommended site blocking should be implemented. Internet policy should be implemented for url filtering and site blocking also.
III. It is strongly recommended antivirus should be installed on all machines which are connected to server.
IV. It is suggested to the organization network monitoring tool should be taken.
V. Currently it is observed that software is remotely accessible from outside the network. This should be restricted.
VI. IP binding and mac binding should be strongly recommended.
VII. Currently it is suggested to the organization DR site should be established and DR drill should be conducted quarterly basis.

DESHPANDE & ASSOCIATES
CHARTERED ACCOUNTANTS
FLAT NO 4, MANISHA APARTMENT, SARASWATINAGAR, NEAR UDYOG BHAVAN,
SANGLI-416416
M 9423829680 O. 0233-2672888
EMAIL: cadeshpandeassociates2006@gmail.com

VIII. Currently it is observe that backup is taken on hard disk and Microsoft one drive. It should be tested periodically.

IX. Pen drives should be disabled on machines where not required as per policy.

X. Network Segregation for internet & non Internet PC should be implemented. This can be done through Layer 3 switch or by using VM ware also.

XI. Antivirus should be installed on all machines.

XII. Crisis Management plan it should be created.

16. FIREWALL CHECKLIST

No.	Security Elements
	Review the rule sets to ensure that they follow the order as follows: anti-spoofing filters (blocked private addresses, internal addresses appearing from the outside) User permit rules (e.g. allow HTTP to public webserver) Management permit rules (e.g. SNMP traps to network management server) Noise drops (e.g. discard OSPF and HSRP chatter) Deny and Alert (alert systems administrator about traffic that is suspicious) Deny and log (log remaining traffic for analysis) Firewalls operate on a first match basis, thus the above structure is important to ensure that suspicious traffic is kept out instead of inadvertently allowing them in by not following the proper order. Remark: Review needs to be conducted for ports and services that are kept open and only those services and ports which are needed as per Cyber Security policy should be kept open.
	Application based firewall Ensure that the administrators monitor any attempts to violate the security policy using the audit logs generated by the application level firewall. Alternatively some application level firewalls provide the functionality to log to intrusion detection systems. In such a

DESHPANDE & ASSOCIATES
CHARTERED ACCOUNTANTS
FLAT NO 4, MANISHA APARTMENT, SARASWATINAGAR, NEAR UDYOG BHAVAN, SANGLI-416416
M 9423829680 O. 0233-2672888
EMAIL: cadeshpandeassociates2006@gmail.com

	circumstance ensure that the correct host, which is hosting the IDS, is defined in the application level firewall. Ensure that there is a process to update the application level firewall's vulnerabilities checked to the most current vulnerabilities. Ensure that there is a process to update the software with the latest attack signatures. In the event of the signatures being downloaded from the vendors' site, ensure that it is a trusted site. In the event of the signature being e-mailed to the systems administrator, ensure that digital signatures are used to verify the vendor and that the information transmitted has not been modified en-route. The following commands should be blocked for SMTP at the application level firewall: EXPN (expand) VRFY (verify) DEBUG WIZARD The following command should be blocked for FTP: PUT Review the denied URL's and ensure that they are appropriate for e.g. any URL's to hacker sites should be blocked. In some instances organizations may want to block access to x-rated sites or other harmful sites. As such they would subscribe to sites, which maintain listings of such harmful sites. Ensure that the URL's to deny are updated as released by the sites that warn of harmful sites. Ensure that only authorized users are authenticated by the application level firewall. Remark: Should be blocked at firewall NAT Policy should be implemented & unnecessary services should be disabled.
	Stateful inspection Review the state tables to ensure that appropriate rules are set up in terms

DESHPANDE & ASSOCIATES
CHARTERED ACCOUNTANTS
FLAT NO 4, MANISHA APARTMENT, SARASWATINAGAR, NEAR UDYOG BHAVAN,
SANGLI-416416
M 9423829680 O. 0233-2672888
EMAIL: cadeshpandeassociates2006@gmail.com

	of source and destination IP's, source and destination ports and timeouts. Ensure that the timeouts are appropriate so as not to give the hacker too much time to launch a successful attack. For URL's If a URL filtering server is used, ensure that it is appropriately defined in the firewall software. If the filtering server is external to the organization ensure that it is a trusted source. If the URL is from a file, ensure that there is adequate protection for this file to ensure no unauthorized modifications. Ensure that specific traffic containing scripts; ActiveX and java are striped prior to being allowed into the internal network. If filtering on MAC addresses is allowed, review the filters to ensure that it is restricted to the appropriate MAC's as defined in the security policy. Remark: URL filtering activity is recommended. Stateful inspection recommended for tracing source ip and port
	Logging and apt blocker: Ensure that logging is enabled and that the logs are reviewed to identify any potential patterns that could indicate an attack. Remark: Should be enabled and apt blocker should be enabled
	Java Control panel security level should be set to high to very high for higher security and control mechanism. This should be implemented on each and every machine. Location – DMZ Ensure that there are two firewalls – one to connect the web server to the internet and the other to connect the web server to the internal network. In the event of two firewalls ensure that it is of different types and that dual NIC's are used. This would increase security since a hacker would need to have knowledge of the strengths, weaknesses and bugs of both firewalls. The rule sets for both firewalls would vary based on their location e.g.

DESHPANDE & ASSOCIATES
CHARTERED ACCOUNTANTS
FLAT NO 4, MANISHA APARTMENT, SARASWATINAGAR, NEAR UDYOG BHAVAN, SANGLI-416416
M 9423829680 O. 0233-2672888
EMAIL: cadeshpandeassociates2006@gmail.com

	between web server and the internet and between web server and the internal network. Remark: Java control panel security status is recommended to very high.
	Vulnerability assessments/ Testing Ascertain if there is a procedure to test for open ports using NMAP and whether unnecessary ports are closed. Ensure that there is a procedure to test the rulesets when established or changed so as not to create a denial of service on the organization or allow any weaknesses to continue undetected. Remark: Nmap test recommended every month. VAPT exercise is recommended yearly
	Compliance with security policy Ensure that the rule set complies with the organization security policy. Remark: Firewall security policy is separately recommended
	Ensure that the following spoofed, private (RFC 1918) and illegal addresses are blocked: Standard unroutables 255.255.255.255 127.0.0.0 Private (RFC 1918) addresses I. 10.0.0.0 – 10.255.255.255 J. 172.16.0.0 – 172.31.255.255 K. 192.168.0.0 - 192.168.255.255 Reserved addresses II. 240.0.0.0 Illegal addresses JJ. 0.0.0.0 UDP echo ICMP broadcast (RFC 2644)

DESHPANDE & ASSOCIATES
CHARTERED ACCOUNTANTS
FLAT NO 4, MANISHA APARTMENT, SARASWATINAGAR, NEAR UDYOG BHAVAN, SANGLI-416416
M 9423829680 O. 0233-2672888
EMAIL: cadeshpandeassociates2006@gmail.com

	Ensure that traffic from the above addresses is not transmitted by the interface. Remark: Recommended
	Ensure that loose source routing and strict source routing (lsrsr & ssrr) are blocked and logged by the firewall. Remark: Recommended
	Port restrictions The following ports should blocked: Above ports are blocked.

Service	Port Type	Port Number
DNS Zone Transfers except from external secondary DNS servers	TCP	53
TFTP Daemon	UDP	69
Link	TCP	87
SUN RPC	TCP & UDP	111
BSD UNIX	TCP	512 – 514
LPD	TCP	515
UUCPD	TCP	540
Open Windows	TCP & UDP	2000
NFS	TCP & UDP	2049
X Windows	TCP & UDP	6000 – 6255
Small services	TCP & UDP	20 and below
FTP	TCP	21
SSH	TCP	22
Telnet	TCP	23
SMTP (except external mail relays)	TCP	25

DESHPANDE & ASSOCIATES
CHARTERED ACCOUNTANTS
FLAT NO 4, MANISHA APARTMENT, SARASWATINAGAR, NEAR UDYOG BHAVAN, SANGLI-416416
M 9423829680 O. 0233-2672888
EMAIL: cadeshpandeassociates2006@gmail.com

NTP	TCP & UDP	37
Finger	TCP	79
HTTP (except to external web servers)	TCP	80
POP	TCP	109 &110
NNTP	TCP	119
NTP	TCP	123
NetBIOS in Windows NT	TCP &UDP	135
NetBIOS in Windows NT	UDP	137 & 138
NetBIOS	TCP	139
IMAP	TCP	143
SNMP	TCP	161 &162
SNMP	UDP	161 &162
BGP	TCP	179
LDAP	TCP &UDP	389
SSL (except to external web servers)	TCP	443
NetBIOS in Win2k	TCP &UDP	445
Syslog	UDP	514
SOCKS	TCP	1080
Cisco AUX port	TCP	2001
Cisco AUX port (stream)	TCP	4001
Lockd (Linux DoS Vulnerability)	TCP &UDP	4045
Cisco AUX port (binary)	TCP	6001
Common high order HTTP ports	TCP	8000, 8080, 8888

Remote access

DESHPANDE & ASSOCIATES
CHARTERED ACCOUNTANTS
FLAT NO 4, MANISHA APARTMENT, SARASWATINAGAR, NEAR UDYOG BHAVAN,
SANGLI-416416
M 9423829680 O. 0233-2672888
EMAIL: cadeshpandeassociates2006@gmail.com

	If remote access is to be used, ensure that the SSH protocol (port 22) is used instead of Telnet. Remark: Recommended
	File Transfers If FTP is a requirement, ensure that the server, which supports FTP, is placed in a different subnet than the internal protected network. Remark: Recommended
	Mail Traffic Ascertain which protocol is used for mail and ensure that there is a rule to block incoming mail traffic except to internal mail. Remark : Dmarc control recommended with highest security configuration
	ICMP (ICMP 8, 11, 3) Ensure that there is a rule blocking ICMP echo requests and replies. Ensure that there is a rule blocking outgoing time exceeded and unreachable messages. Remark: Should be Blocked.
	IP Readdressing/IP Masquerading Ensure that the firewall rules have the readdressing option enabled such that internal IP addresses are not displayed to the external untrusted networks. Remark: Recommended

Network admin, system admin and database admin roles and responsibilities.

DESHPANDE & ASSOCIATES
CHARTERED ACCOUNTANTS
FLAT NO 4 , MANISHA APARTMENT ,SARASWATINAGAR, NEAR UDYOG BHAVAN , SANGLI-416416
M 9423829680 O. 0233-2672888
EMAIL : cadeshpandeassociates2006@gmail.com
audit-admin@cadeshpandeassociates.com
Website: www.cadeshpandeassociates.com

DATA CENTER INSPECTION REPORT

AUDIT CONDUCTED BY:

DESHPANDE & ASSOCIATES

Mr. Dheeraj Deshpande (B.com, FCA,DISA,CISA)

Mr. Nitin Kedar (B Com)

Audit representatives from the Organization:

Mr. Randive (IT Manager)
Mr. Prasanna (IT Staff)

DESHPANDE & ASSOCIATES
CHARTERED ACCOUNTANTS
FLAT NO 4 , MANISHA APARTMENT ,SARASWATINAGAR, NEAR UDYOG BHAVAN , SANGLI-416416
M 9423829680 O. 0233-2672888
EMAIL : cadeshpandeassociates2006@gmail.com
audit-admin@cadeshpandeassociates.com
Website: www.cadeshpandeassociates.com

We are enclosing herewith the detailed report containing our remarks and suggestions regarding Data Center hardware, networking and other issues.
Kindly give compliance to issues where control is inadequate within 30 days.
Thanks & Regards

For Deshpande & Associates
Chartered Accountants

Dheeraj Deshpande
FCA, CISA, DISA
Date : 12/07/2022

DESHPANDE & ASSOCIATES
CHARTERED ACCOUNTANTS
FLAT NO 4 , MANISHA APARTMENT ,SARASWATINAGAR, NEAR UDYOG BHAVAN , SANGLI-416416
M 9423829680 O. 0233-2672888
EMAIL : cadeshpandeassociates2006@gmail.com
audit-admin@cadeshpandeassociates.com
Website: www.cadeshpandeassociates.com

DATA CENTRE	AUDIT PROGRAM: DATE OF INSPECTION : 20/06/2022

Step	Audit Procedure	REMARK	CONTROL ADEQUATE Y/N
	BACKGROUND & PLANNING		
1.	Obtain adequate background information on the audit area such as: 1. Productivity and performance measurement reports/stats (i.e. uptime percentage, etc) 2. Equipment maintenance, monitoring and/or testing documentation (i.e. generator, fire suppression, battery testing, etc) 3. Policies & Procedures 4. List of information technology applications utilized 5. List of laws and regulations 6. Data Center diagram 7. Organizational chart 8. Inventory listing	1. Up time % set at 99.99 %. Observed and down time recording is not done. 2. Fire suppression Device not available at DC site. 3. Not Available 4. Equipment documentation is not available. 5. PCI DSS laws and regulations set needed at the DC and it should be studied and updated by the IT staff. 6. Data center diagram is prepared. 7. Not Available 8. Available	1. Yes 2. No 3. No 4. No 5. No 6. Yes 7. No 8. Yes

DESHPANDE & ASSOCIATES
CHARTERED ACCOUNTANTS
FLAT NO 4 , MANISHA APARTMENT ,SARASWATINAGAR, NEAR UDYOG BHAVAN , SANGLI-416416
M 9423829680 O. 0233-2672888
EMAIL : cadeshpandeassociates2006@gmail.com
audit-admin@cadeshpandeassociates.com
Website: www.cadeshpandeassociates.com

2.	Review policies and procedures for completeness verifying they at a minimum address compliance with laws and regulations. Also consider the following: • Does a data center security policy exist, and is the policy current and adequately detailed? • Do access authorization procedures exist and do the procedures apply to all persons (e.g., employees and vendors) requiring access to the data center? • Do equipment maintenance and testing policies exist?	• No • Access authorization procedures not defined and documented. • Scheduled equipment maintenance is on Call basis but documentation should be kept.	• No • Yes • No
3.	Examine productivity and performance measures for trends to assist in the developing audit scope.	Following measures should be defined and tested as per benchmarks: 1. Data back-up time 15 Minute Approx. 2. Data restoration time 15.00 Minute 3. HIM Database server Backup size 3 GB approx. Biometric log server size 5 Gb approx.	As per remark
4.	Review financial reports/statements for unusual trends/fluctuations (i.e. budget stats such as maintenance and purchases versus actual).	Any fluctuation as per standard and actual should be reported to IT manager regarding IT related activities and to CEO regarding financial activities.	Yes

DESHPANDE & ASSOCIATES
CHARTERED ACCOUNTANTS
FLAT NO 4 , MANISHA APARTMENT ,SARASWATINAGAR, NEAR UDYOG BHAVAN , SANGLI-416416
M 9423829680 O. 0233-2672888
EMAIL : cadeshpandeassociates2006@gmail.com
audit-admin@cadeshpandeassociates.com
Website: www.cadeshpandeassociates.com

5.	Arrange a tour of the data center and observe, consider and/or inquire about the following: 1. Is the data center location conspicuous 2. Is access controlled via locks, monitoring devices, etc 3. Usage of uninterruptible power supplies (UPS), battery backups, and generators 4. Temperature control and/or monitoring devices 5. Air conditioner control and/or monitoring devices 6. Rodent devices 7. Are evacuation plans/maps posted 8. Is wire/cabling kept orderly and are server cabinets locked? 9. Is CCTV installed & monitored at DC ?	1. Yes 2. Bio-metric access not available. 3. 1 UPS 10 KVA available and 20 Batteries 6 hours back up. is available and tested. 4. Not available 5. Available 6. Rodent device not available. 7. No available 8. Orderly cabling available & only locked cabinets available. 9. CCTV not available at DC.	1. Yes 2. No 3. Yes 4. No 5. Yes 6. No 7. No 8. Yes 9. Yes
INFORMATION SYSTEMS			
The following represents general information systems test work to be performed if warranted based on the risk posed by individual systems.			
6.	Determine and list the primary information systems utilized within the operations. Consider performing the following testing based on the risk.	No such primary information system arrangement. It should be prepared for all software and hardware based primary information systems.	No
7.	Review the process for granting and terminating user access. Perform detailed testing to determine if access is terminated timely.	Reviewed	Yes

DESHPANDE & ASSOCIATES
CHARTERED ACCOUNTANTS
FLAT NO 4 , MANISHA APARTMENT ,SARASWATINAGAR, NEAR UDYOG BHAVAN , SANGLI-416416
M 9423829680 O. 0233-2672888
EMAIL : cadeshpandeassociates2006@gmail.com
audit-admin@cadeshpandeassociates.com
Website: www.cadeshpandeassociates.com

8.	On a sample basis, test specific user access to determine if access is commensurate with job functions. Additionally, determine if access promotes adequate segregation of duties.	User parameters are tested for access rights & privileges. Currently it is possible to determine how many users are allotted system admin role, how many users are allotted computer operator role. Role wise parameters are already defined in the system.	Reviewed
9.	Perform testing where necessary to determine if system data is adequately backed up.	Scheduled Back up is taken daily at 11 PM on One Drive.	Yes. Reviewed
10.	Determine the nature and extent of system interfaces. Review (perform testing of) interfaces to determine if data is accurate, complete and timely. Also consider whether there is a process to address interface errors.	NA	
11.	Determine the effectiveness of basic application controls. Consider the following: Does the system • Promote the use of strong passwords • Contain an appropriate audit trail • Contain adequate input validation controls	 • Password policy is not available. • Available but not monitored. • Check as per application software report	 • No • No • No
	PHYSICAL ACCESS		

DESHPANDE & ASSOCIATES
CHARTERED ACCOUNTANTS
FLAT NO 4 , MANISHA APARTMENT ,SARASWATINAGAR, NEAR UDYOG BHAVAN , SANGLI-416416
M 9423829680 O. 0233-2672888
EMAIL : cadeshpandeassociates2006@gmail.com
audit-admin@cadeshpandeassociates.com
Website: www.cadeshpandeassociates.com

12.	After completing the tour of the Data Center, describe physical access controls. Consider the following: • Is access limited to individuals whose primary business functions require them to have access • Does the unit maintain access reports documenting individuals who have accessed the data center (including date and time) • Are these reports reviewed on a regular basis • Does the business unit maintain a visitors log and are visitors escorted by authorized individuals	• IT Team allowed to DC • Register should be maintained. • No • Register is not maintained	
13.	Obtain a listing of individuals with access to the data center. Perform detailed audit testing to attain reasonable assurance that user access is appropriate.	Prepared such list, user rights should be approved by organization.	
14.	Review time/date stamped access list for specified time period for unusual access activity (i.e. unusual times, frequency, etc).	Logs are kept	
15.	Obtain a listing of individuals with access to the wire/telecom closets. Perform detailed audit testing to attain reasonable assurance that user access is appropriate.	Such list should be maintained.	
16.	Ensure closed circuit television (CCTVs) system data, if applicable, is backed up appropriately and in a manner that allows relatively easy retrieval.	In the data center CCTV not installed.	No
	ASSET PROTECTION AND PRESERVATION		
17.	Determine the nature of fire suppression and/or control mechanisms (i.e. wet pipe, dry pipe, Halon OR CO^2) and the corresponding policies and procedures utilized.	Fire extinguisher is not available, only for DC. Temperature control Device should be installed.	No
	α) Determine if shutdown procedures are documented and disseminated to employees.	Register should be maintained. Policy and procedures should be prepared.	No

DESHPANDE & ASSOCIATES
CHARTERED ACCOUNTANTS
FLAT NO 4 , MANISHA APARTMENT ,SARASWATINAGAR, NEAR UDYOG BHAVAN , SANGLI-416416
M 9423829680 O. 0233-2672888
EMAIL : cadeshpandeassociates2006@gmail.com
audit-admin@cadeshpandeassociates.com
Website: www.cadeshpandeassociates.com

	β) Evaluate the fire detection and reaction systems and procedures: • Determine if inspections, testing, and practice drills are performed by reviewing any logs/documentation.	Fire Detection is not available.	No
18.	Determine the nature and extent of temperature controls and monitoring mechanisms.	Temperature monitoring should be installed. Alarm system should be installed for DC.	
	a) Ensure only authorized person can access temperature controls.	Access control not implemented.	
	b) Determine if monitoring mechanisms provide reasonable assurance that relevant personnel will be alerted of temperature changes in a timely fashion.	Alarm system alert disabled.	
19.	Determine the extent, usage and maintenance of electrical power. For example, does the data center use UPS systems, battery backup and/or generators. If so, how are they used?		
	α) UPS	Yes	
	β) Regarding the battery—Gain an understanding of how much power is needed and for how long. Ensure the current battery satisfies the objective.	6 hour battery backup	
	χ) Determine if the battery is tested periodically. Examine test records.	On call basis tested and report is not maintained.	
	δ) If maintenance (recharging, etc) is required, review records to ensure maintenance occurs as needed.	Records is maintained.	
	ε) Regarding the generator—Gain an understanding of how much power is needed and for how long. Ensure the current generator satisfies the objective.	NA	
	ϕ) Determine if the generator is tested periodically. Examine test records.	Generator is available	
	γ) If maintenance (refueling, etc) is required, review records to ensure maintenance occurs as needed.	Record facility is not applied.	
MEDIA MANAGEMENT/BACK UP & RECOVERY			

DESHPANDE & ASSOCIATES
CHARTERED ACCOUNTANTS
FLAT NO 4 , MANISHA APARTMENT ,SARASWATINAGAR, NEAR UDYOG BHAVAN , SANGLI-416416
M 9423829680 O. 0233-2672888
EMAIL : cadeshpandeassociates2006@gmail.com
audit-admin@cadeshpandeassociates.com
Website: www.cadeshpandeassociates.com

20.	Gain a general understanding of the media management processes including gaining reasonable assurance: • There is adequate access to removable media • There is a sufficient backup process covering critical data that enables timely recovery of said data. • Determine if data is encrypted.	1. Yes 2. Mirroring is not available at database level. 3. Stored data is encrypted at database level.	
21.	Obtain the review the backup schedule or log. Determine if backups occur on a consistent basis and cover all servers containing critical data. Obtain explanations for lapses in backup activity.	Scheduled backup exercise is taken daily 11 PM.	
22. e	Regarding onsite storage – Obtain an understanding of media aging and rotation, cataloging and check in/out procedures. If necessary, perform inventory testing by selecting a sample of items from the inventory and tracing to the catalogue and vice versa. Ensure appropriate security of storage media both on premises and during transit.	No such process Inventory information filling in the system is not done. During transit security must be enabled	No
23.	Obtain and review check in/out logs. • Determine if items shipped to and received from others are appropriately logged. • Compare shipping details to backup schedule in order to evaluate backup/shipping lag time.	Reviewed	No

DESHPANDE & ASSOCIATES
CHARTERED ACCOUNTANTS
FLAT NO 4 , MANISHA APARTMENT ,SARASWATINAGAR, NEAR UDYOG BHAVAN , SANGLI-416416
M 9423829680 O. 0233-2672888
EMAIL : cadeshpandeassociates2006@gmail.com
audit-admin@cadeshpandeassociates.com
Website: www.cadeshpandeassociates.com

24.	Obtain an understanding of the offsite storage processes and inspect how they are managed. Specifically, Examine the contract and determine if it addresses/contains the following: • A right to audit clause • Description of the type of support provided (i.e. turnaround times, etc) • Security and environmental controls	Offsite Storage Process implemented. Authorized person should be defined with whom external back up data should be stored.	Yes
25.	If necessary, visit the offsite storage facility and assess: • Facility security • Cataloging and storage methodologies • Environmental security	Offsite storage facility is enabled.	NA
	α) Additionally, perform detailed testing of the process by: • Selecting items from the floor and tracing them to the catalogue • Selecting items from the catalogue and tracing them to the floor • Selecting items from the data center's log marked as "delivered" and trace to the offsite storage provider's records. Ensure deliveries are timely.	Done Done offsite storage available	No
	INVENTORY MANAGEMENT		
26.	Gain an understanding of the inventory management processes.	Checked.	
27.	Obtain an inventory listing from the appropriate party (i.e. IT, Fixed Assets, etc).	Checked. List is not prepared.	
28.	If significant technology assets exists, perform detailed testing to ensure assets are appropriately accounted for (i.e. this may include receiving, storing and retirement processes. Additionally, it may include performing an inventory count on a sample basis.	Checked	

DESHPANDE & ASSOCIATES
CHARTERED ACCOUNTANTS
FLAT NO 4 , MANISHA APARTMENT ,SARASWATINAGAR, NEAR UDYOG BHAVAN , SANGLI-416416
M 9423829680 O. 0233-2672888
EMAIL : cadeshpandeassociates2006@gmail.com
audit-admin@cadeshpandeassociates.com
Website: www.cadeshpandeassociates.com

SIGNIFICANT ASSETS OUTSIDE OF DATA CENTER			
29.	Determine the extent of information technology hardware maintained outside of the official data center.	Checked as per EDP record	
30.	If applicable, perform details testing to determine if these assets are adequately safeguarded, properly accounted for, and sufficiently protected from environment risks. Use testing methods similar to those describe above for data center operations.	Adequate technology is adopted and it should be used properly. New Asset acquisition & installation procedure should be established and followed as per IT policy.	
OTHER			
31.	Where outsourced and/or in sourced processes exist, obtain and review relevant service level agreement and ensure it records the common understanding about services, priorities, responsibilities, etc.	• No such out sourced process. • Comprehensive insurance cover should be taken to cope up Data Center Hardware and if possible of DATA. • Agreement made between vendor and university is valid one on a ground of stamp duty	
WRAP UP			
32.	Note all issues on the issue log.	Logs are maintained but not monitored. It should be monitor on daily.	
33.	Submit work papers for review.	Submitted and discussed with IT staff.	

DESHPANDE & ASSOCIATES
CHARTERED ACCOUNTANTS
FLAT NO 4 , MANISHA APARTMENT ,SARASWATINAGAR, NEAR UDYOG BHAVAN , SANGLI-416416
M 9423829680 O. 0233-2672888
EMAIL : cadeshpandeassociates2006@gmail.com
audit-admin@cadeshpandeassociates.com
Website: www.cadeshpandeassociates.com

General Points:

Both server warranty is ened on
Application Server: 04/02/2020

Database Server: 08/10/2019
Immediate action should be taken.

1. We advise the organization to undertake separate cyber insurance policy for Data Center. At data center back up should be scheduled at periodic intervals. Instead of taking back up at day end back up should be done as per that schedule.

2. Currently vendor has access at DC but no logs are maintained for the same. Access logs should be maintained.

3. A log in the form of screen recording should be maintained of the changes made by software vendor at the back end.

4. Exceptional transaction log & parameters changes log is available through system to IT manager but not monitor, it should be monitor daily.

5. Desktop sharing facility should be license copy installed and recording should be strictly available in software.

1 Application

Total Space : 2.8 TB Used : 33 GB Free Space : 2.05 TB
Lenovo RAID 530 8i SCSI
Procesor : Intel (R) Xeon (R) Silver 4110 CPU @ 2.10GHz, 2095Mhz,8 Core(S) 16 Logical

1 Database
64 GB RAM
Processor : Intel® Silver 4110 CPU @ 2.10GHz 64 bit

DESHPANDE & ASSOCIATES
CHARTERED ACCOUNTANTS
FLAT NO 4 , MANISHA APARTMENT ,SARASWATINAGAR, NEAR UDYOG BHAVAN , SANGLI-416416
M 9423829680 O. 0233-2672888
EMAIL : cadeshpandeassociates2006@gmail.com
audit-admin@cadeshpandeassociates.com
Website: www.cadeshpandeassociates.com

Lenovo RAID 530 8i SCSI
OS : Windows Server 2016 Standard
Ram : 32GB
Processor : Intel® Xeon ® Silver 4110 CPU @ 2.10 GHz 2.10 GHz

DESHPANDE & ASSOCIATES
CHARTERED ACCOUNTANTS
ADDRESS: FLAT NO 4, MANISHA APARTMENT, SARASWATINAGAR, NEAR UDYOG BHAVAN, SANGLI-416416 M 9423829680 O. 0233-2672888
EMAIL: cadeshpandeassociates2006@gmail.com
Website: www.cadeshpandeassociates.com

VAPT (VULNERABILITY ASSESSMENT PENETRATION TESTING) REPORT

ORGNIZATION NAME:- DR. D Y PATIL EDUCATION SOCIETY, KOLHAPUR

ADDRESS:,A/P/ KOLHAPUR DIST KOLHAPUR

EXECUTIVE SUMMARY

Date : 25/06/2022

To,

Dr. D Y Patil Education Society,

Kolhapur

District: Kolhapur

Sub: Regarding Submission of VAPT report of your Orgnization

Respected Sir,

As per your communication dated, 06/05/2022 we have conducted the VAPT audit of your Orgnization .

We are submitting herewith audit report with detailed findings and recommendations for your kind appraisal.

Kindly acknowledge the same.

For Deshpande & Associates
Chartered Accountants

Dheeraj Deshpande
Date : 25/06/2022

DESHPANDE & ASSOCIATES * Chartered Accountants * FRN 136235W

DESHPANDE & ASSOCIATES
CHARTERED ACCOUNTANTS
ADDRESS: FLAT NO 4, MANISHA APARTMENT, SARASWATINAGAR, NEAR UDYOG BHAVAN, SANGLI-416416 M 9423829680 O. 0233-2672888
EMAIL: cadeshpandeassociates2006@gmail.com
Website: www.cadeshpandeassociates.com

DETAILS OF FINDING & RECOMMENDATIONS:

1. IP Address: 14.139.120.66

Nmap Scan Report - Scanned at Tue Jun 14 10:40:03 2022

- **Scan Summary**

- | **14.139.120.66**

Scan Summary

Nmap 7.70 was initiated at Tue Jun 14 10:40:03 2022 with these arguments:
nmap -sV --stats-every 10s --max-retries=3 --min-rtt-timeout 100ms --max-rtt-timeout 1000ms --initial-rtt-timeout 200ms --host-timeout 240m --min-rate 12 -T3 14.139.120.66

Verbosity: 0; Debug level 0

Nmap done at Tue Jun 14 10:40:35 2022; 1 IP address (1 host up) scanned in 32.15 seconds

14.139.120.66

Address

- 14.139.120.66 (ipv4)

Ports

The 998 ports scanned but not shown below are in state: **filtered**

- 998 ports replied with: **no-responses**

Port		State (toggle closed [0] | filtered [0])	Service	Reason	Product	Version	Extra info
222	tcp	open	ssh	syn-ack	OpenSSH	7.9	protocol

DESHPANDE & ASSOCIATES
CHARTERED ACCOUNTANTS
ADDRESS: FLAT NO 4, MANISHA APARTMENT, SARASWATINAGAR, NEAR UDYOG BHAVAN, SANGLI-416416 M 9423829680 O. 0233-2672888
EMAIL: cadeshpandeassociates2006@gmail.com
Website: www.cadeshpandeassociates.com

							2.0
443	tcp	open	http	syn-ack	Apache httpd		

Misc Metrics (click to expand)

2. IP Address : 14.139.120.70

Nmap Scan Report - Scanned at Tue Jun 14 10:41:38 2022

- **Scan Summary**
- | **14.139.120.70**

Scan Summary

Nmap 7.70 was initiated at Tue Jun 14 10:41:38 2022 with these arguments:
nmap -sV --stats-every 10s --max-retries=3 --min-rtt-timeout 100ms --max-rtt-timeout 1000ms --initial-rtt-timeout 200ms --host-timeout 240m --min-rate 12 -T3 14.139.120.70

Verbosity: 0; Debug level 0

Nmap done at Tue Jun 14 10:42:03 2022; 1 IP address (1 host up) scanned in 25.98 seconds

14.139.120.70

Address

- 14.139.120.70 (ipv4)

Ports

The 996 ports scanned but not shown below are in state: **filtered**

- 996 ports replied with: **no-responses**

DESHPANDE & ASSOCIATES
CHARTERED ACCOUNTANTS
ADDRESS: FLAT NO 4, MANISHA APARTMENT, SARASWATINAGAR, NEAR UDYOG BHAVAN, SANGLI-416416 M 9423829680 O. 0233-2672888
EMAIL: cadeshpandeassociates2006@gmail.com
Website: www.cadeshpandeassociates.com

Port		State (toggle closed [2] | filtered [0])	Service	Reason	Product	Version	Extra info
21	tcp	open	ftp	syn-ack	vsftpd	2.0.8 or later	
80	tcp	open	http	syn-ack	Apache httpd	2.4.7	(Ubuntu)

Misc Metrics (click to expand)

3. IP Address: 14.139.120.71

Nmap Scan Report - Scanned at Tue Jun 14 10:41:48 2022

- **Scan Summary**

- **| 14.139.120.71**

Scan Summary

Nmap 7.70 was initiated at Tue Jun 14 10:41:48 2022 with these arguments:
nmap -sV --stats-every 10s --max-retries=3 --min-rtt-timeout 100ms --max-rtt-timeout 1000ms --initial-rtt-timeout 200ms --host-timeout 240m --min-rate 12 -T3 14.139.120.71

Verbosity: 0; Debug level 0

Nmap done at Tue Jun 14 10:42:29 2022; 1 IP address (1 host up) scanned in 41.02 seconds

14.139.120.71

Address

- 14.139.120.71 (ipv4)

Ports

DESHPANDE & ASSOCIATES
CHARTERED ACCOUNTANTS
ADDRESS: FLAT NO 4, MANISHA APARTMENT, SARASWATINAGAR, NEAR UDYOG BHAVAN, SANGLI-416416 M 9423829680 O. 0233-2672888
EMAIL: cadeshpandeassociates2006@gmail.com
Website: www.cadeshpandeassociates.com

The 923 ports scanned but not shown below are in state: **filtered**

- 923 ports replied with: **no-responses**

The 74 ports scanned but not shown below are in state: **closed**

- 74 ports replied with: **resets**

Port		State (toggle closed [0] | filtered [0])	Service	Reason	Product	Version	Extra info
82	tcp	Open	http	syn-ack	Microsoft IIS httpd	8.5	
443	tcp	Open	http	syn-ack	Apache Tomcat/Coyote JSP engine	1.1	
10003	tcp	Open	documentum_s	syn-ack			

Misc Metrics (click to expand)

4. IP Address : 14.139.120.76

Nmap Scan Report - Scanned at Tue Jun 14 10:42:39 2022

- **Scan Summary**

- **\| 14.139.120.76**

Scan Summary

Nmap 7.70 was initiated at Tue Jun 14 10:42:39 2022 with these arguments:
nmap -sV --stats-every 10s --max-retries=3 --min-rtt-timeout 100ms --max-rtt-timeout 1000ms --initial-rtt-timeout 200ms --host-timeout 240m --min-rate 12 -T3 14.139.120.76

DESHPANDE & ASSOCIATES
CHARTERED ACCOUNTANTS
ADDRESS: FLAT NO 4, MANISHA APARTMENT, SARASWATINAGAR, NEAR UDYOG BHAVAN, SANGLI-416416 M 9423829680 O. 0233-2672888
EMAIL: cadeshpandeassociates2006@gmail.com
Website: www.cadeshpandeassociates.com

Verbosity: 0; Debug level 0

Nmap done at Tue Jun 14 10:43:12 2022; 1 IP address (1 host up) scanned in 33.13 seconds

14.139.120.76

Address

- 14.139.120.76 (ipv4)

Ports

The 999 ports scanned but not shown below are in state: **filtered**

- 999 ports replied with: **no-responses**

Port		State (toggle closed [0] | filtered [0])	Service	Reason	Product	Version	Extra info
443	tcp	Open	http	syn-ack	SonicWALL firewall http config		

Misc Metrics (click to expand)

DESHPANDE & ASSOCIATES
CHARTERED ACCOUNTANTS
ADDRESS: FLAT NO 4, MANISHA APARTMENT, SARASWATINAGAR, NEAR UDYOG BHAVAN, SANGLI-416416 M 9423829680 O. 0233-2672888
EMAIL: cadeshpandeassociates2006@gmail.com
Website: www.cadeshpandeassociates.com

Open VAS scanner Findings & Recommendations:

1. IP Address : 14.139.120.66

Summary

This document reports on the results of an automatic security scan. The report first summarises the results found. Then, for each host, the report describes every issue found. Please consider the advice given in each description, in order to rectify the issue.

This report might not show details of all issues that were found. Issues with the threat level "Debug" are not shown. Issues with the threat level "False Positive" are not shown. Only results with a minimum QoD of 70 are shown.

All dates are displayed using the timezone "Coordinated Universal Time", which is abbreviated "UTC".

Scan started:	Tue Jun 14 16:08:41 2022
Scan ended:	Tue Jun 14 17:25:10 2022
Task:	Scan of 14.139.120.66

Host Summary

Host	Start	End	High	Medium	Low	Log	False Positive
14.139.120.66	Jun 14, 16:09:31	Jun 14, 17:25:04	1	3	1	25	0
Total: 0			1	3	1	25	0

Results per Host

Host 14.139.120.66

DESHPANDE & ASSOCIATES
CHARTERED ACCOUNTANTS
ADDRESS: FLAT NO 4, MANISHA APARTMENT, SARASWATINAGAR, NEAR UDYOG BHAVAN, SANGLI-416416 M 9423829680 O. 0233-2672888
EMAIL: cadeshpandeassociates2006@gmail.com
Website: www.cadeshpandeassociates.com

Scanning of this host started at:	Tue Jun 14 16:09:31 2022
Number of results:	30

Port Summary for Host 14.139.120.66

Service (Port)	Threat Level
general/CPE-T	Log
general/tcp	Log
222/tcp	Log
443/tcp	High

Security Issues for Host 14.139.120.66

443/tcp

Medium (CVSS: 4.3)

NVT: Apache HTTP Server 'httpOnly' Cookie Information Disclosure Vulnerability (OID: 1.3.6.1.4.1.25623.1.0.902830)

Product detection result: cpe:/a:apache:http_server by Apache HTTP Server Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.117232)

Summary

Apache HTTP Server is prone to a cookie information disclosure vulnerability.

Vulnerability Detection Result

Vulnerability was detected according to the Vulnerability Detection Method.

Impact

Successful exploitation will allow attackers to obtain sensitive information that may aid in further attacks.

Solution

DESHPANDE & ASSOCIATES
CHARTERED ACCOUNTANTS
ADDRESS: FLAT NO 4, MANISHA APARTMENT, SARASWATINAGAR, NEAR UDYOG BHAVAN, SANGLI-416416 M 9423829680 O. 0233-2672888
EMAIL: cadeshpandeassociates2006@gmail.com
Website: www.cadeshpandeassociates.com

Solution type: VendorFix

Update to Apache HTTP Server version 2.2.22 or later.

Affected Software/OS

Apache HTTP Server versions 2.2.0 through 2.2.21.

Vulnerability Insight

The flaw is due to an error within the default error response for status code 400 when no custom ErrorDocument is configured, which can be exploited to expose 'httpOnly' cookies.

Vulnerability Detection Method

Details: Apache HTTP Server 'httpOnly' Cookie Information Disclosure Vulnerability (OID: 1.3.6.1.4.1.25623.1.0.902830)

Version used: 2022-04-27T12:01:52Z

Product Detection Result

Product:	cpe:/a:apache:http_server
Method:	Apache HTTP Server Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.117232)

References

CVE:	CVE-2012-0053
Other:	http://secunia.com/advisories/47779
	http://www.securityfocus.com/bid/51706
	http://www.exploit-db.com/exploits/18442
	http://rhn.redhat.com/errata/RHSA-2012-0128.html
	http://httpd.apache.org/security/vulnerabilities_22.html
	http://svn.apache.org/viewvc?view=revision&revision=1235454
	http://lists.opensuse.org/opensuse-security-announce/2012-02/msg00026.html
CERT:	CB-K15/0080, CB-K14/1505, CB-K14/0608, DFN-CERT-2015-0082, DFN-CERT-2014-1592, DFN-CERT-2014-0635, DFN-CERT-2013-1307, DFN-CERT-2012-1276, DFN-CERT-2012-1112, DFN-CERT-2012-0928, DFN-CERT-2012-0758, DFN-CERT-2012-0744, DFN-CERT-2012-0568, DFN-CERT-2012-0425, DFN-CERT-

DESHPANDE & ASSOCIATES
CHARTERED ACCOUNTANTS
ADDRESS: FLAT NO 4, MANISHA APARTMENT, SARASWATINAGAR, NEAR UDYOG BHAVAN, SANGLI-416416 M 9423829680 O. 0233-2672888
EMAIL: cadeshpandeassociates2006@gmail.com
Website: www.cadeshpandeassociates.com

	2012-0424, DFN-CERT-2012-0387, DFN-CERT-2012-0343, DFN-CERT-2012-0332, DFN-CERT-2012-0306, DFN-CERT-2012-0264, DFN-CERT-2012-0203, DFN-CERT-2012-0188

443/tcp

Medium (CVSS: 5.0)

NVT: SSL/TLS: Certificate Expired (OID: 1.3.6.1.4.1.25623.1.0.103955)

Summary

The remote server's SSL/TLS certificate has already expired.

Vulnerability Detection Result

The certificate of the remote service expired on 2020-09-09 12:24:24.

Certificate details:
fingerprint (SHA-1) | 1CCA23772872AE7D73F5C5F1DD3B5C4AB9B79FFF
fingerprint (SHA-256) | FF7D98FC7ED441E26C4B8B8440235A3E971B641BFA41A4BCE2CB368CD25E4AF3
issued by | 1.2.840.113549.1.9.1=#737570706F72744067616A736869656C642E636F6D,CN=ca.gajshield.com,OU=IT,O=Gajshield Infotech Pvt. Ltd,L=Mumbai,ST=Maharashtra,C=IN
public key size (bits) | 4096
serial | 00E38E55509C78A122
signature algorithm | sha256WithRSAEncryption
subject | 1.2.840.113549.1.9.1=#737570706F72744067616A736869656C642E636F6D,CN=fw2.gajshield.com,OU=IT,O=Gajshield Infotech Pvt. Ltd.,L=Mumbai,ST=Maharastra,C=IN
subject alternative names (SAN) | fw2.gajshield.com
valid from | 2018-09-10 12:24:24 UTC
valid until | 2020-09-09 12:24:24 UTC

Solution

Solution type: Mitigation

Replace the SSL/TLS certificate by a new one.

DESHPANDE & ASSOCIATES
CHARTERED ACCOUNTANTS
ADDRESS: FLAT NO 4, MANISHA APARTMENT, SARASWATINAGAR, NEAR UDYOG BHAVAN, SANGLI-416416 M 9423829680 O. 0233-2672888
EMAIL: cadeshpandeassociates2006@gmail.com
Website: www.cadeshpandeassociates.com

Vulnerability Insight

This script checks expiry dates of certificates associated with SSL/TLS-enabled services on the target and reports whether any have already expired.

Vulnerability Detection Method

Details: SSL/TLS: Certificate Expired (OID: 1.3.6.1.4.1.25623.1.0.103955)

Version used: 2021-11-22T15:32:39Z

443/tcp

Medium (CVSS: 4.3)

NVT: SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection (OID: 1.3.6.1.4.1.25623.1.0.117274)

Summary

It was possible to detect the usage of the deprecated TLSv1.0 and/or TLSv1.1 protocol on this system.

Vulnerability Detection Result

The service is only providing the deprecated TLSv1.0 protocol and supports one or more ciphers. Those supported ciphers can be found in the 'SSL/TLS: Report Supported Cipher Suites' (OID: 1.3.6.1.4.1.25623.1.0.802067) VT.

Impact

An attacker might be able to use the known cryptographic flaws to eavesdrop the connection between clients and the service to get access to sensitive data transferred within the secured connection.

Furthermore newly uncovered vulnerabilities in this protocols won't receive security updates anymore.

DESHPANDE & ASSOCIATES
CHARTERED ACCOUNTANTS
ADDRESS: FLAT NO 4, MANISHA APARTMENT, SARASWATINAGAR, NEAR UDYOG BHAVAN, SANGLI-416416 M 9423829680 O. 0233-2672888
EMAIL: cadeshpandeassociates2006@gmail.com
Website: www.cadeshpandeassociates.com

Solution

Solution type: Mitigation

It is recommended to disable the deprecated TLSv1.0 and/or TLSv1.1 protocols in favor of the TLSv1.2+ protocols. Please see the references for more information.

Affected Software/OS

All services providing an encrypted communication using the TLSv1.0 and/or TLSv1.1 protocols.

Vulnerability Insight

The TLSv1.0 and TLSv1.1 protocols contain known cryptographic flaws like:

- CVE-2011-3389: Browser Exploit Against SSL/TLS (BEAST)

- CVE-2015-0204: Factoring Attack on RSA-EXPORT Keys Padding Oracle On Downgraded Legacy Encryption (FREAK)

Vulnerability Detection Method

Check the used TLS protocols of the services provided by this system.

Details: SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection (OID: 1.3.6.1.4.1.25623.1.0.117274)

Version used: 2021-07-19T08:11:48Z

References

CVE:	CVE-2011-3389, CVE-2015-0204
Other:	https://ssl-config.mozilla.org/
	https://bettercrypto.org/
	https://datatracker.ietf.org/doc/rfc8996/
	https://vnhacker.blogspot.com/2011/09/beast.html
	https://web.archive.org/web/20201108095603/https://censys.io/blog/freak

	https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters-report-2014
CERT:	CB-K18/0799, CB-K16/1289, CB-K16/1096, CB-K15/1751, CB-K15/1266, CB-K15/0850, CB-K15/0764, CB-K15/0720, CB-K15/0548, CB-K15/0526, CB-K15/0509, CB-K15/0493, CB-K15/0384, CB-K15/0365, CB-K15/0364, CB-K15/0302, CB-K15/0192, CB-K15/0079, CB-K15/0016, CB-K14/1342, CB-K14/0231, CB-K13/0845, CB-K13/0796, CB-K13/0790, DFN-CERT-2020-0177, DFN-CERT-2020-0111, DFN-CERT-2019-0068, DFN-CERT-2018-1441, DFN-CERT-2018-1408, DFN-CERT-2016-1372, DFN-CERT-2016-1164, DFN-CERT-2016-0388, DFN-CERT-2015-1853, DFN-CERT-2015-1332, DFN-CERT-2015-0884, DFN-CERT-2015-0800, DFN-CERT-2015-0758, DFN-CERT-2015-0567, DFN-CERT-2015-0544, DFN-CERT-2015-0530, DFN-CERT-2015-0396, DFN-CERT-2015-0375, DFN-CERT-2015-0374, DFN-CERT-2015-0305, DFN-CERT-2015-0199, DFN-CERT-2015-0079, DFN-CERT-2015-0021, DFN-CERT-2014-1414, DFN-CERT-2013-1847, DFN-CERT-2013-1792, DFN-CERT-2012-1979, DFN-CERT-2012-1829, DFN-CERT-2012-1530, DFN-CERT-2012-1380, DFN-CERT-2012-1377, DFN-CERT-2012-1292, DFN-CERT-2012-1214, DFN-CERT-2012-1213, DFN-CERT-2012-1180, DFN-CERT-2012-1156, DFN-CERT-2012-1155, DFN-CERT-2012-1039, DFN-CERT-2012-0956, DFN-CERT-2012-0908, DFN-CERT-2012-0868, DFN-CERT-2012-0867, DFN-CERT-2012-0848, DFN-CERT-2012-0838, DFN-CERT-2012-0776, DFN-CERT-2012-0722, DFN-CERT-2012-0638, DFN-CERT-2012-0627, DFN-CERT-2012-0451, DFN-CERT-2012-0418, DFN-CERT-2012-0354, DFN-CERT-2012-0234, DFN-CERT-2012-0221, DFN-CERT-2012-0177, DFN-CERT-2012-0170, DFN-CERT-2012-0146, DFN-CERT-2012-0142, DFN-CERT-2012-0126, DFN-CERT-2012-0123, DFN-CERT-2012-0095, DFN-CERT-2012-0051, DFN-CERT-2012-0047, DFN-CERT-2012-0021, DFN-CERT-2011-1953, DFN-CERT-2011-1946, DFN-CERT-2011-1844, DFN-CERT-2011-1826, DFN-CERT-2011-1774, DFN-CERT-2011-1743, DFN-CERT-2011-1738, DFN-CERT-2011-1706, DFN-CERT-2011-1628, DFN-CERT-2011-1627, DFN-CERT-2011-1619, DFN-CERT-2011-1482

443/tcp

High (CVSS: 7.4)

NVT: SSL/TLS: OpenSSL CCS Man in the Middle Security Bypass Vulnerability (OID: 1.3.6.1.4.1.25623.1.0.105042)

Summary

DESHPANDE & ASSOCIATES
CHARTERED ACCOUNTANTS
ADDRESS: FLAT NO 4, MANISHA APARTMENT, SARASWATINAGAR, NEAR UDYOG BHAVAN, SANGLI-416416 M 9423829680 O. 0233-2672888
EMAIL: cadeshpandeassociates2006@gmail.com
Website: www.cadeshpandeassociates.com

OpenSSL is prone to security-bypass vulnerability.

Vulnerability Detection Result

Vulnerability was detected according to the Vulnerability Detection Method.

Impact

Successfully exploiting this issue may allow attackers to obtain sensitive information by conducting a man-in-the-middle attack. This may lead to other attacks.

Solution

Solution type: VendorFix

Updates are available. Please see the references for more information.

Affected Software/OS

OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m and 1.0.1 before 1.0.1h.

Vulnerability Insight

OpenSSL does not properly restrict processing of ChangeCipherSpec messages, which allows man-in-the-middle attackers to trigger use of a zero-length master key in certain OpenSSL-to-OpenSSL communications, and consequently hijack sessions or obtain sensitive information, via a crafted TLS handshake, aka the 'CCS Injection' vulnerability.

Vulnerability Detection Method

Send two SSL ChangeCipherSpec request and check the response.

Details: SSL/TLS: OpenSSL CCS Man in the Middle Security Bypass Vulnerability (OID: 1.3.6.1.4.1.25623.1.0.105042)

Version used: 2022-04-14T11:24:11Z

References

DESHPANDE & ASSOCIATES
CHARTERED ACCOUNTANTS
ADDRESS: FLAT NO 4, MANISHA APARTMENT, SARASWATINAGAR, NEAR UDYOG BHAVAN, SANGLI-416416 M 9423829680 O. 0233-2672888
EMAIL: cadeshpandeassociates2006@gmail.com
Website: www.cadeshpandeassociates.com

CVE:	CVE-2014-0224
Other:	https://www.openssl.org/news/secadv/20140605.txt
	http://www.securityfocus.com/bid/67899
CERT:	CB-K15/0567, CB-K15/0415, CB-K15/0384, CB-K15/0080, CB-K15/0079, CB-K15/0074, CB-K14/1617, CB-K14/1537, CB-K14/1299, CB-K14/1297, CB-K14/1294, CB-K14/1202, CB-K14/1174, CB-K14/1153, CB-K14/0876, CB-K14/0756, CB-K14/0746, CB-K14/0736, CB-K14/0722, CB-K14/0716, CB-K14/0708, CB-K14/0684, CB-K14/0683, CB-K14/0680, DFN-CERT-2016-0388, DFN-CERT-2015-0593, DFN-CERT-2015-0427, DFN-CERT-2015-0396, DFN-CERT-2015-0082, DFN-CERT-2015-0079, DFN-CERT-2015-0078, DFN-CERT-2014-1717, DFN-CERT-2014-1632, DFN-CERT-2014-1364, DFN-CERT-2014-1357, DFN-CERT-2014-1350, DFN-CERT-2014-1265, DFN-CERT-2014-1209, DFN-CERT-2014-0917, DFN-CERT-2014-0789, DFN-CERT-2014-0778, DFN-CERT-2014-0768, DFN-CERT-2014-0752, DFN-CERT-2014-0747, DFN-CERT-2014-0738, DFN-CERT-2014-0715, DFN-CERT-2014-0714, DFN-CERT-2014-0709

2. **IP Address : 14.139.120.67**
1. **IP Address : 14.12.139.70**

Summary

This document reports on the results of an automatic security scan. The report first summarises the results found. Then, for each host, the report describes every issue found. Please consider the advice given in each description, in order to rectify the issue.

This report might not show details of all issues that were found. Issues with the threat level "Debug" are not shown. Issues with the threat level "False Positive" are not shown. Only results with a minimum QoD of 70 are shown.

All dates are displayed using the timezone "Coordinated Universal Time", which is abbreviated "UTC".

Scan started:	Tue Jun 14 16:19:41 2022
Scan ended:	Tue Jun 14 16:54:09 2022
Task:	Scan of 14.139.120.70

Host Summary

DESHPANDE & ASSOCIATES
CHARTERED ACCOUNTANTS
ADDRESS: FLAT NO 4, MANISHA APARTMENT, SARASWATINAGAR, NEAR UDYOG BHAVAN, SANGLI-416416 M 9423829680 O. 0233-2672888
EMAIL: cadeshpandeassociates2006@gmail.com
Website: www.cadeshpandeassociates.com

Host	Start	End	High	Medium	Low	Log	False Positive
14.139.120.70	Jun 14, 16:20:45	Jun 14, 16:54:06	0	2	1	16	0
Total: 0			0	2	1	16	0

Results per Host

Host 14.139.120.70

Scanning of this host started at:	Tue Jun 14 16:20:45 2022
Number of results:	19

Port Summary for Host 14.139.120.70

Service (Port)	Threat Level
21/tcp	Medium
80/tcp	Log
general/CPE-T	Log
general/tcp	Low

Security Issues for Host 14.139.120.70

21/tcp

Medium (CVSS: 6.4)

NVT: Anonymous FTP Login Reporting (OID: 1.3.6.1.4.1.25623.1.0.900600)

Summary

Reports if the remote FTP Server allows anonymous logins.

Vulnerability Detection Result

It was possible to login to the remote FTP service with the following anonymous account(s):

anonymous:anonymous@example.com

DESHPANDE & ASSOCIATES
CHARTERED ACCOUNTANTS
ADDRESS: FLAT NO 4, MANISHA APARTMENT, SARASWATINAGAR, NEAR UDYOG BHAVAN, SANGLI-416416 M 9423829680 O. 0233-2672888
EMAIL: cadeshpandeassociates2006@gmail.com
Website: www.cadeshpandeassociates.com

ftp:anonymous@example.com

Here are the contents of the remote FTP directory listing:

Account "anonymous":

```
-rw-r--r--   1 0      0       3562898 Dec 01  2018 feedback_17_18_sem_II_graph.zip
-rw-r--r--   1 0      0        197797 Jul 16  2018 maxresdefault.jpg
```

Account "ftp":

```
-rw-r--r--   1 0      0       3562898 Dec 01  2018 feedback_17_18_sem_II_graph.zip
-rw-r--r--   1 0      0        197797 Jul 16  2018 maxresdefault.jpg
```

Impact

Based on the files accessible via this anonymous FTP login and the permissions of this account an attacker might be able to:

- gain access to sensitive files

- upload or delete files.

Solution

Solution type: Mitigation

If you do not want to share files, you should disable anonymous logins.

Vulnerability Insight

A host that provides an FTP service may additionally provide Anonymous FTP access as well. Under this arrangement, users do not strictly need an account on the host. Instead the user typically enters 'anonymous' or 'ftp' when prompted for username. Although users are commonly asked to send their email address as their password, little to no verification is actually performed on the supplied data.

DESHPANDE & ASSOCIATES
CHARTERED ACCOUNTANTS
ADDRESS: FLAT NO 4, MANISHA APARTMENT, SARASWATINAGAR, NEAR UDYOG BHAVAN, SANGLI-416416 M 9423829680 O. 0233-2672888
EMAIL: cadeshpandeassociates2006@gmail.com
Website: www.cadeshpandeassociates.com

Remark: NIST don't see 'configuration issues' as software flaws so the referenced CVE has a severity of 0.0. The severity of this VT has been raised by Greenbone to still report a configuration issue on the target.

Vulnerability Detection Method

Details: Anonymous FTP Login Reporting (OID: 1.3.6.1.4.1.25623.1.0.900600)

Version used: 2021-10-20T09:03:29Z

References

CVE:	CVE-1999-0497

21/tcp

Medium (CVSS: 4.8)

NVT: FTP Unencrypted Cleartext Login (OID: 1.3.6.1.4.1.25623.1.0.108528)

Summary

The remote host is running a FTP service that allows cleartext logins over unencrypted connections.

Vulnerability Detection Result

The remote FTP service accepts logins without a previous sent 'AUTH TLS' command. Response(s):

Non-anonymous sessions: 331 Please specify the password.
Anonymous sessions: 331 Please specify the password.

Impact

An attacker can uncover login names and passwords by sniffing traffic to the FTP service.

Solution

DESHPANDE & ASSOCIATES
CHARTERED ACCOUNTANTS
ADDRESS: FLAT NO 4, MANISHA APARTMENT, SARASWATINAGAR, NEAR UDYOG BHAVAN, SANGLI-416416 M 9423829680 O. 0233-2672888
EMAIL: cadeshpandeassociates2006@gmail.com
Website: www.cadeshpandeassociates.com

Solution type: Mitigation

Enable FTPS or enforce the connection via the 'AUTH TLS' command. Please see the manual of the FTP service for more information.

Vulnerability Detection Method

Tries to login to a non FTPS enabled FTP service without sending a 'AUTH TLS' command first and checks if the service is accepting the login without enforcing the use of the 'AUTH TLS' command.

Details: FTP Unencrypted Cleartext Login (OID: 1.3.6.1.4.1.25623.1.0.108528)

Version used: 2020-08-24T08:40:10Z

3. IP Address : 14.139.120.71

Summary

This document reports on the results of an automatic security scan. The report first summarises the results found. Then, for each host, the report describes every issue found. Please consider the advice given in each description, in order to rectify the issue.

This report might not show details of all issues that were found. Issues with the threat level "Debug" are not shown. Issues with the threat level "False Positive" are not shown. Only results with a minimum QoD of 70 are shown.

All dates are displayed using the timezone "Coordinated Universal Time", which is abbreviated "UTC".

Scan started:	Tue Jun 14 16:26:27 2022
Scan ended:	Tue Jun 14 17:44:10 2022
Task:	Scan of 14.139.120.71

Host Summary

DESHPANDE & ASSOCIATES
CHARTERED ACCOUNTANTS
ADDRESS: FLAT NO 4, MANISHA APARTMENT, SARASWATINAGAR, NEAR UDYOG BHAVAN, SANGLI-416416 M 9423829680 O. 0233-2672888
EMAIL: cadeshpandeassociates2006@gmail.com
Website: www.cadeshpandeassociates.com

Host	Start	End	High	Medium	Low	Log	False Positive
14.139.120.71	Jun 14, 16:27:40	Jun 14, 17:44:03	0	5	1	40	0
Total: 0			0	5	1	40	0

Results per Host

Host 14.139.120.71

Scanning of this host started at:	Tue Jun 14 16:27:40 2022
Number of results:	46

Port Summary for Host 14.139.120.71

Service (Port)	Threat Level
5006/tcp	Medium
general/CPE-T	Log
10003/tcp	Log
82/tcp	Medium
443/tcp	Medium
general/tcp	Low
5005/tcp	Log

Security Issues for Host 14.139.120.71

82/tcp

Medium (CVSS: 5.0)

NVT: Microsoft IIS Tilde Character Information Disclosure Vulnerability (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.802887)

Product detection result: cpe:/a:microsoft:internet_information_services:8.5 by Microsoft Internet Information Services (IIS) Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.900710)

Summary

DESHPANDE & ASSOCIATES
CHARTERED ACCOUNTANTS
ADDRESS: FLAT NO 4, MANISHA APARTMENT, SARASWATINAGAR, NEAR UDYOG BHAVAN, SANGLI-416416 M 9423829680 O. 0233-2672888
EMAIL: cadeshpandeassociates2006@gmail.com
Website: www.cadeshpandeassociates.com

The Microsoft IIS Webserver is prone to an information disclosure vulnerability.

Vulnerability Detection Result

File/Folder name found on server starting with:

aspnet

enumerated based on the following HTTP responses:

- Received a "HTTP 400 (Bad Request)" status code or a "0x80070002" error code when accessing the invalid File/Folder "1234567890" via the URL:
http://14.139.120.71:82/%2F1234567890*1~*%2Fa.aspx?aspxerrorpath=/

- Received a "HTTP 404 (Not Found)" status code or a "0x00000000" error code when accessing a valid File/Folder with the following subsequent enumeration requests:
http://14.139.120.71:82/%2Fa*~1*%2Fa.aspx?aspxerrorpath=/
http://14.139.120.71:82/%2Fas*~1*%2Fa.aspx?aspxerrorpath=/
http://14.139.120.71:82/%2Fasp*~1*%2Fa.aspx?aspxerrorpath=/
http://14.139.120.71:82/%2Faspn*~1*%2Fa.aspx?aspxerrorpath=/
http://14.139.120.71:82/%2Faspne*~1*%2Fa.aspx?aspxerrorpath=/
http://14.139.120.71:82/%2Faspnet*~1*%2Fa.aspx?aspxerrorpath=/

Impact

Successful exploitation will allow remote attackers to obtain sensitive information that could aid in further attacks.

Solution

Solution type: WillNotFix

No known solution was made available for at least one year since the disclosure of this vulnerability. Likely none will be provided anymore. General solution options are to upgrade to a newer release, disable respective features, remove the product or replace the product by another one.

Affected Software/OS

All versions of the Microsoft IIS Webserver.

DESHPANDE & ASSOCIATES
CHARTERED ACCOUNTANTS
ADDRESS: FLAT NO 4, MANISHA APARTMENT, SARASWATINAGAR, NEAR UDYOG BHAVAN, SANGLI-416416 M 9423829680 O. 0233-2672888
EMAIL: cadeshpandeassociates2006@gmail.com
Website: www.cadeshpandeassociates.com

Vulnerability Insight

Microsoft IIS fails to validate a specially crafted GET request containing a '~' tilde character, which allows to disclose all short-names of folders and files having 4 letters extensions.

Vulnerability Detection Method

Sends various crafted HTTP GET requests and checks the responses.

Details: Microsoft IIS Tilde Character Information Disclosure Vulnerability (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.802887)

Version used: 2022-04-27T12:01:52Z

Product Detection Result

Product:	cpe:/a:microsoft:internet_information_services:8.5
Method:	Microsoft Internet Information Services (IIS) Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.900710)

References

Other:	http://www.exploit-db.com/exploits/19525
	http://www.securityfocus.com/bid/54251
	http://code.google.com/p/iis-shortname-scanner-poc
	http://soroush.secproject.com/downloadable/iis_tilde_shortname_disclosure.txt
	http://soroush.secproject.com/downloadable/microsoft_iis_tilde_character_vulnerability_feature.pdf

5006/tcp

Medium (CVSS: 5.0)

NVT: Missing `httpOnly` Cookie Attribute (OID: 1.3.6.1.4.1.25623.1.0.105925)

Summary

The application is missing the 'httpOnly' cookie attribute

DESHPANDE & ASSOCIATES
CHARTERED ACCOUNTANTS
ADDRESS: FLAT NO 4, MANISHA APARTMENT, SARASWATINAGAR, NEAR UDYOG BHAVAN, SANGLI-416416 M 9423829680 O. 0233-2672888
EMAIL: cadeshpandeassociates2006@gmail.com
Website: www.cadeshpandeassociates.com

Vulnerability Detection Result

The cookies:

Set-Cookie: ASPSESSIONIDAABBSBBQ=***replaced***; path=/

are missing the "httpOnly" attribute.

Solution

Solution type: Mitigation

Set the 'httpOnly' attribute for any session cookie.

Affected Software/OS

Application with session handling in cookies.

Vulnerability Insight

The flaw is due to a cookie is not using the 'httpOnly' attribute. This allows a cookie to be accessed by JavaScript which could lead to session hijacking attacks.

Vulnerability Detection Method

Check all cookies sent by the application for a missing 'httpOnly' attribute

Details: Missing `httpOnly` Cookie Attribute (OID: 1.3.6.1.4.1.25623.1.0.105925)

Version used: 2020-08-24T15:18:35Z

References

Other:	https://www.owasp.org/index.php/HttpOnly
	https://www.owasp.org/index.php/Testing_for_cookies_attributes_(OTG-SESS-002)

443/tcp

Medium (CVSS: 4.3)

DESHPANDE & ASSOCIATES
CHARTERED ACCOUNTANTS
ADDRESS: FLAT NO 4, MANISHA APARTMENT, SARASWATINAGAR, NEAR UDYOG BHAVAN, SANGLI-416416 M 9423829680 O. 0233-2672888
EMAIL: cadeshpandeassociates2006@gmail.com
Website: www.cadeshpandeassociates.com

NVT: SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection (OID: 1.3.6.1.4.1.25623.1.0.117274)

Summary

It was possible to detect the usage of the deprecated TLSv1.0 and/or TLSv1.1 protocol on this system.

Vulnerability Detection Result

The service is only providing the deprecated TLSv1.0 protocol and supports one or more ciphers. Those supported ciphers can be found in the 'SSL/TLS: Report Supported Cipher Suites' (OID: 1.3.6.1.4.1.25623.1.0.802067) VT.

Impact

An attacker might be able to use the known cryptographic flaws to eavesdrop the connection between clients and the service to get access to sensitive data transferred within the secured connection.

Furthermore newly uncovered vulnerabilities in this protocols won't receive security updates anymore.

Solution

Solution type: Mitigation

It is recommended to disable the deprecated TLSv1.0 and/or TLSv1.1 protocols in favor of the TLSv1.2+ protocols. Please see the references for more information.

Affected Software/OS

All services providing an encrypted communication using the TLSv1.0 and/or TLSv1.1 protocols.

Vulnerability Insight

The TLSv1.0 and TLSv1.1 protocols contain known cryptographic flaws like:

DESHPANDE & ASSOCIATES
CHARTERED ACCOUNTANTS
ADDRESS: FLAT NO 4, MANISHA APARTMENT, SARASWATINAGAR, NEAR UDYOG BHAVAN, SANGLI-416416 M 9423829680 O. 0233-2672888
EMAIL: cadeshpandeassociates2006@gmail.com
Website: www.cadeshpandeassociates.com

- CVE-2011-3389: Browser Exploit Against SSL/TLS (BEAST)

- CVE-2015-0204: Factoring Attack on RSA-EXPORT Keys Padding Oracle On Downgraded Legacy Encryption (FREAK)

Vulnerability Detection Method

Check the used TLS protocols of the services provided by this system.

Details: SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection (OID: 1.3.6.1.4.1.25623.1.0.117274)

Version used: 2021-07-19T08:11:48Z

References

CVE:	CVE-2011-3389, CVE-2015-0204
Other:	https://ssl-config.mozilla.org/
	https://bettercrypto.org/
	https://datatracker.ietf.org/doc/rfc8996/
	https://vnhacker.blogspot.com/2011/09/beast.html
	https://web.archive.org/web/20201108095603/https://censys.io/blog/freak
	https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters-report-2014
CERT:	CB-K18/0799, CB-K16/1289, CB-K16/1096, CB-K15/1751, CB-K15/1266, CB-K15/0850, CB-K15/0764, CB-K15/0720, CB-K15/0548, CB-K15/0526, CB-K15/0509, CB-K15/0493, CB-K15/0384, CB-K15/0365, CB-K15/0364, CB-K15/0302, CB-K15/0192, CB-K15/0079, CB-K15/0016, CB-K14/1342, CB-K14/0231, CB-K13/0845, CB-K13/0796, CB-K13/0790, DFN-CERT-2020-0177, DFN-CERT-2020-0111, DFN-CERT-2019-0068, DFN-CERT-2018-1441, DFN-CERT-2018-1408, DFN-CERT-2016-1372, DFN-CERT-2016-1164, DFN-CERT-2016-0388, DFN-CERT-2015-1853, DFN-CERT-2015-1332, DFN-CERT-2015-0884, DFN-CERT-2015-0800, DFN-CERT-2015-0758, DFN-CERT-2015-0567, DFN-CERT-2015-0544, DFN-CERT-2015-0530, DFN-CERT-2015-0396, DFN-CERT-2015-0375, DFN-CERT-2015-0374, DFN-CERT-2015-0305, DFN-CERT-2015-0199, DFN-CERT-2015-0079, DFN-CERT-2015-0021, DFN-CERT-2014-1414, DFN-CERT-2013-1847, DFN-CERT-2013-1792, DFN-CERT-2012-1979, DFN-CERT-2012-1829, DFN-CERT-2012-1530, DFN-CERT-2012-1380, DFN-CERT-2012-1377, DFN-CERT-2012-1292, DFN-CERT-2012-1214, DFN-CERT-2012-1213, DFN-CERT-2012-1180, DFN-CERT-

DESHPANDE & ASSOCIATES
CHARTERED ACCOUNTANTS
ADDRESS: FLAT NO 4, MANISHA APARTMENT, SARASWATINAGAR, NEAR UDYOG BHAVAN, SANGLI-416416 M 9423829680 O. 0233-2672888
EMAIL: cadeshpandeassociates2006@gmail.com
Website: www.cadeshpandeassociates.com

	2012-1156, DFN-CERT-2012-1155, DFN-CERT-2012-1039, DFN-CERT-2012-0956, DFN-CERT-2012-0908, DFN-CERT-2012-0868, DFN-CERT-2012-0867, DFN-CERT-2012-0848, DFN-CERT-2012-0838, DFN-CERT-2012-0776, DFN-CERT-2012-0722, DFN-CERT-2012-0638, DFN-CERT-2012-0627, DFN-CERT-2012-0451, DFN-CERT-2012-0418, DFN-CERT-2012-0354, DFN-CERT-2012-0234, DFN-CERT-2012-0221, DFN-CERT-2012-0177, DFN-CERT-2012-0170, DFN-CERT-2012-0146, DFN-CERT-2012-0142, DFN-CERT-2012-0126, DFN-CERT-2012-0123, DFN-CERT-2012-0095, DFN-CERT-2012-0051, DFN-CERT-2012-0047, DFN-CERT-2012-0021, DFN-CERT-2011-1953, DFN-CERT-2011-1946, DFN-CERT-2011-1844, DFN-CERT-2011-1826, DFN-CERT-2011-1774, DFN-CERT-2011-1743, DFN-CERT-2011-1738, DFN-CERT-2011-1706, DFN-CERT-2011-1628, DFN-CERT-2011-1627, DFN-CERT-2011-1619, DFN-CERT-2011-1482

443/tcp

Medium (CVSS: 4.0)

NVT: SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerabili... (OID: 1.3.6.1.4.1.25623.1.0.106223)

Summary

The SSL/TLS service uses Diffie-Hellman groups with insufficient strength (key size < 2048).

Vulnerability Detection Result

Server Temporary Key Size: 1024 bits

Impact

An attacker might be able to decrypt the SSL/TLS communication offline.

Solution

Solution type: Workaround

Deploy (Ephemeral) Elliptic-Curve Diffie-Hellman (ECDHE) or use a 2048-bit or stronger Diffie-Hellman group (see the references).

DESHPANDE & ASSOCIATES
CHARTERED ACCOUNTANTS
ADDRESS: FLAT NO 4, MANISHA APARTMENT, SARASWATINAGAR, NEAR UDYOG BHAVAN, SANGLI-416416 M 9423829680 O. 0233-2672888
EMAIL: cadeshpandeassociates2006@gmail.com
Website: www.cadeshpandeassociates.com

For Apache Web Servers: Beginning with version 2.4.7, mod_ssl will use DH parameters which include primes with lengths of more than 1024 bits.

Vulnerability Insight

The Diffie-Hellman group are some big numbers that are used as base for the DH computations. They can be, and often are, fixed. The security of the final secret depends on the size of these parameters. It was found that 512 and 768 bits to be weak, 1024 bits to be breakable by really powerful attackers like governments.

Vulnerability Detection Method

Checks the DHE temporary public key size.

Details: SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerabili... (OID: 1.3.6.1.4.1.25623.1.0.106223)

Version used: 2021-02-12T06:42:15Z

References

Other:	https://weakdh.org/
	https://weakdh.org/sysadmin.html

443/tcp

Medium (CVSS: 5.0)

NVT: SSL/TLS: Report Weak Cipher Suites (OID: 1.3.6.1.4.1.25623.1.0.103440)

Summary

This routine reports all Weak SSL/TLS cipher suites accepted by a service.

NOTE: No severity for SMTP services with 'Opportunistic TLS' and weak cipher suites on port 25/tcp is reported. If too strong cipher suites are configured for this service the alternative would be to fall back to an even more insecure cleartext communication.

DESHPANDE & ASSOCIATES
CHARTERED ACCOUNTANTS
ADDRESS: FLAT NO 4, MANISHA APARTMENT, SARASWATINAGAR, NEAR UDYOG BHAVAN, SANGLI-416416 M 9423829680 O. 0233-2672888
EMAIL: cadeshpandeassociates2006@gmail.com
Website: www.cadeshpandeassociates.com

Vulnerability Detection Result

'Weak' cipher suites accepted by this service via the TLSv1.0 protocol:

TLS_RSA_WITH_SEED_CBC_SHA

Solution

Solution type: Mitigation

The configuration of this services should be changed so that it does not accept the listed weak cipher suites anymore.

Please see the references for more resources supporting you with this task.

Vulnerability Insight

These rules are applied for the evaluation of the cryptographic strength:

- RC4 is considered to be weak (CVE-2013-2566, CVE-2015-2808)

- Ciphers using 64 bit or less are considered to be vulnerable to brute force methods and therefore considered as weak (CVE-2015-4000)

- 1024 bit RSA authentication is considered to be insecure and therefore as weak

- Any cipher considered to be secure for only the next 10 years is considered as medium

- Any other cipher is considered as strong

Vulnerability Detection Method

Details: SSL/TLS: Report Weak Cipher Suites (OID: 1.3.6.1.4.1.25623.1.0.103440)

Version used: 2021-12-01T13:10:37Z

References

DESHPANDE & ASSOCIATES
CHARTERED ACCOUNTANTS
ADDRESS: FLAT NO 4, MANISHA APARTMENT, SARASWATINAGAR, NEAR UDYOG BHAVAN, SANGLI-416416 M 9423829680 O. 0233-2672888
EMAIL: cadeshpandeassociates2006@gmail.com
Website: www.cadeshpandeassociates.com

CVE:	CVE-2013-2566, CVE-2015-2808, CVE-2015-4000
Other:	https://www.bsi.bund.de/SharedDocs/Warnmeldungen/DE/CB/warnmeldung_cb-k16-1465_update_6.html
	https://bettercrypto.org/
	https://mozilla.github.io/server-side-tls/ssl-config-generator/
CERT:	CB-K21/0067, CB-K19/0812, CB-K17/1750, CB-K16/1593, CB-K16/1552, CB-K16/1102, CB-K16/0617, CB-K16/0599, CB-K16/0168, CB-K16/0121, CB-K16/0090, CB-K16/0030, CB-K15/1751, CB-K15/1591, CB-K15/1550, CB-K15/1517, CB-K15/1514, CB-K15/1464, CB-K15/1442, CB-K15/1334, CB-K15/1269, CB-K15/1136, CB-K15/1090, CB-K15/1059, CB-K15/1022, CB-K15/1015, CB-K15/0986, CB-K15/0964, CB-K15/0962, CB-K15/0932, CB-K15/0927, CB-K15/0926, CB-K15/0907, CB-K15/0901, CB-K15/0896, CB-K15/0889, CB-K15/0877, CB-K15/0850, CB-K15/0849, CB-K15/0834, CB-K15/0827, CB-K15/0802, CB-K15/0764, CB-K15/0733, CB-K15/0667, CB-K14/0935, CB-K13/0942, DFN-CERT-2021-0775, DFN-CERT-2020-1561, DFN-CERT-2020-1276, DFN-CERT-2017-1821, DFN-CERT-2016-1692, DFN-CERT-2016-1648, DFN-CERT-2016-1168, DFN-CERT-2016-0665, DFN-CERT-2016-0642, DFN-CERT-2016-0184, DFN-CERT-2016-0135, DFN-CERT-2016-0101, DFN-CERT-2016-0035, DFN-CERT-2015-1853, DFN-CERT-2015-1679, DFN-CERT-2015-1632, DFN-CERT-2015-1608, DFN-CERT-2015-1542, DFN-CERT-2015-1518, DFN-CERT-2015-1406, DFN-CERT-2015-1341, DFN-CERT-2015-1194, DFN-CERT-2015-1144, DFN-CERT-2015-1113, DFN-CERT-2015-1078, DFN-CERT-2015-1067, DFN-CERT-2015-1038, DFN-CERT-2015-1016, DFN-CERT-2015-1012, DFN-CERT-2015-0980, DFN-CERT-2015-0977, DFN-CERT-2015-0976, DFN-CERT-2015-0960, DFN-CERT-2015-0956, DFN-CERT-2015-0944, DFN-CERT-2015-0937, DFN-CERT-2015-0925, DFN-CERT-2015-0884, DFN-CERT-2015-0881, DFN-CERT-2015-0879, DFN-CERT-2015-0866, DFN-CERT-2015-0844, DFN-CERT-2015-0800, DFN-CERT-2015-0737, DFN-CERT-2015-0696, DFN-CERT-2014-0977

4. IP Address : 14.139.120.75

Summary

This document reports on the results of an automatic security scan. The report first summarises the results found. Then, for each host, the report describes every issue found. Please consider the advice given in each description, in order to rectify the issue.

DESHPANDE & ASSOCIATES
CHARTERED ACCOUNTANTS
ADDRESS: FLAT NO 4, MANISHA APARTMENT, SARASWATINAGAR, NEAR UDYOG BHAVAN, SANGLI-416416 M 9423829680 O. 0233-2672888
EMAIL: cadeshpandeassociates2006@gmail.com
Website: www.cadeshpandeassociates.com

This report might not show details of all issues that were found. Issues with the threat level "Debug" are not shown. Issues with the threat level "False Positive" are not shown. Only results with a minimum QoD of 70 are shown.

All dates are displayed using the timezone "Coordinated Universal Time", which is abbreviated "UTC".

Scan started:	Tue Jun 14 17:02:05 2022
Scan ended:	Tue Jun 14 18:03:22 2022
Task:	Scan of 14.139.120.75

Host Summary

Host	Start	End	High	Medium	Low	Log	False Positive
14.139.120.75 (hmis.dypunik.edu.in)	Jun 14, 17:03:09	Jun 14, 18:03:20	1	1	0	28	0
Total: 0			1	1	0	28	0

Results per Host

Host 14.139.120.75

Scanning of this host started at:	Tue Jun 14 17:03:09 2022
Number of results:	30

Port Summary for Host 14.139.120.75

Service (Port)	Threat Level
general/CPE-T	Log
80/tcp	Log
443/tcp	High
general/tcp	Log

Security Issues for Host 14.139.120.75

DESHPANDE & ASSOCIATES
CHARTERED ACCOUNTANTS
ADDRESS: FLAT NO 4, MANISHA APARTMENT, SARASWATINAGAR, NEAR UDYOG BHAVAN, SANGLI-416416 M 9423829680 O. 0233-2672888
EMAIL: cadeshpandeassociates2006@gmail.com
Website: www.cadeshpandeassociates.com

Medium (CVSS: 4.3)

NVT: SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection (OID: 1.3.6.1.4.1.25623.1.0.117274)

Summary

It was possible to detect the usage of the deprecated TLSv1.0 and/or TLSv1.1 protocol on this system.

Vulnerability Detection Result

In addition to TLSv1.2+ the service is also providing the deprecated TLSv1.0 and TLSv1.1 protocols and supports one or more ciphers. Those supported ciphers can be found in the 'SSL/TLS: Report Supported Cipher Suites' (OID: 1.3.6.1.4.1.25623.1.0.802067) VT.

Impact

An attacker might be able to use the known cryptographic flaws to eavesdrop the connection between clients and the service to get access to sensitive data transferred within the secured connection.

Furthermore newly uncovered vulnerabilities in this protocols won't receive security updates anymore.

Solution

Solution type: Mitigation

It is recommended to disable the deprecated TLSv1.0 and/or TLSv1.1 protocols in favor of the TLSv1.2+ protocols. Please see the references for more information.

Affected Software/OS

All services providing an encrypted communication using the TLSv1.0 and/or TLSv1.1 protocols.

Vulnerability Insight

The TLSv1.0 and TLSv1.1 protocols contain known cryptographic flaws like:

DESHPANDE & ASSOCIATES
CHARTERED ACCOUNTANTS
ADDRESS: FLAT NO 4, MANISHA APARTMENT, SARASWATINAGAR, NEAR UDYOG BHAVAN, SANGLI-416416 M 9423829680 O. 0233-2672888
EMAIL: cadeshpandeassociates2006@gmail.com
Website: www.cadeshpandeassociates.com

- CVE-2011-3389: Browser Exploit Against SSL/TLS (BEAST)

- CVE-2015-0204: Factoring Attack on RSA-EXPORT Keys Padding Oracle On Downgraded Legacy Encryption (FREAK)

Vulnerability Detection Method

Check the used TLS protocols of the services provided by this system.

Details: SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection (OID: 1.3.6.1.4.1.25623.1.0.117274)

Version used: 2021-07-19T08:11:48Z

References

CVE:	CVE-2011-3389, CVE-2015-0204
Other:	https://ssl-config.mozilla.org/
	https://bettercrypto.org/
	https://datatracker.ietf.org/doc/rfc8996/
	https://vnhacker.blogspot.com/2011/09/beast.html
	https://web.archive.org/web/20201108095603/https://censys.io/blog/freak
	https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters-report-2014
CERT:	CB-K18/0799, CB-K16/1289, CB-K16/1096, CB-K15/1751, CB-K15/1266, CB-K15/0850, CB-K15/0764, CB-K15/0720, CB-K15/0548, CB-K15/0526, CB-K15/0509, CB-K15/0493, CB-K15/0384, CB-K15/0365, CB-K15/0364, CB-K15/0302, CB-K15/0192, CB-K15/0079, CB-K15/0016, CB-K14/1342, CB-K14/0231, CB-K13/0845, CB-K13/0796, CB-K13/0790, DFN-CERT-2020-0177, DFN-CERT-2020-0111, DFN-CERT-2019-0068, DFN-CERT-2018-1441, DFN-CERT-2018-1408, DFN-CERT-2016-1372, DFN-CERT-2016-1164, DFN-CERT-2016-0388, DFN-CERT-2015-1853, DFN-CERT-2015-1332, DFN-CERT-2015-0884, DFN-CERT-2015-0800, DFN-CERT-2015-0758, DFN-CERT-2015-0567, DFN-CERT-2015-0544, DFN-CERT-2015-0530, DFN-CERT-2015-0396, DFN-CERT-2015-0375, DFN-CERT-2015-0374, DFN-CERT-2015-0305, DFN-CERT-2015-0199, DFN-CERT-2015-0079, DFN-CERT-2015-0021, DFN-CERT-2014-1414, DFN-CERT-2013-1847, DFN-CERT-2013-1792, DFN-CERT-2012-1979, DFN-CERT-2012-1829, DFN-CERT-2012-1530, DFN-CERT-2012-1380, DFN-CERT-2012-1377, DFN-CERT-2012-1292, DFN-CERT-2012-1214, DFN-CERT-2012-1213, DFN-CERT-2012-1180, DFN-CERT-

DESHPANDE & ASSOCIATES
CHARTERED ACCOUNTANTS
ADDRESS: FLAT NO 4, MANISHA APARTMENT, SARASWATINAGAR, NEAR UDYOG BHAVAN, SANGLI-416416 M 9423829680 O. 0233-2672888
EMAIL: cadeshpandeassociates2006@gmail.com
Website: www.cadeshpandeassociates.com

	2012-1156, DFN-CERT-2012-1155, DFN-CERT-2012-1039, DFN-CERT-2012-0956, DFN-CERT-2012-0908, DFN-CERT-2012-0868, DFN-CERT-2012-0867, DFN-CERT-2012-0848, DFN-CERT-2012-0838, DFN-CERT-2012-0776, DFN-CERT-2012-0722, DFN-CERT-2012-0638, DFN-CERT-2012-0627, DFN-CERT-2012-0451, DFN-CERT-2012-0418, DFN-CERT-2012-0354, DFN-CERT-2012-0234, DFN-CERT-2012-0221, DFN-CERT-2012-0177, DFN-CERT-2012-0170, DFN-CERT-2012-0146, DFN-CERT-2012-0142, DFN-CERT-2012-0126, DFN-CERT-2012-0123, DFN-CERT-2012-0095, DFN-CERT-2012-0051, DFN-CERT-2012-0047, DFN-CERT-2012-0021, DFN-CERT-2011-1953, DFN-CERT-2011-1946, DFN-CERT-2011-1844, DFN-CERT-2011-1826, DFN-CERT-2011-1774, DFN-CERT-2011-1743, DFN-CERT-2011-1738, DFN-CERT-2011-1706, DFN-CERT-2011-1628, DFN-CERT-2011-1627, DFN-CERT-2011-1619, DFN-CERT-2011-1482

443/tcp

High (CVSS: 7.5)

NVT: SSL/TLS: Report Vulnerable Cipher Suites for HTTPS (OID: 1.3.6.1.4.1.25623.1.0.108031)

Summary

This routine reports all SSL/TLS cipher suites accepted by a service where attack vectors exists only on HTTPS services.

Vulnerability Detection Result

'Vulnerable' cipher suites accepted by this service via the TLSv1.0 protocol:

TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)

'Vulnerable' cipher suites accepted by this service via the TLSv1.1 protocol:

TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)

'Vulnerable' cipher suites accepted by this service via the TLSv1.2 protocol:

TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)

DESHPANDE & ASSOCIATES
CHARTERED ACCOUNTANTS
ADDRESS: FLAT NO 4, MANISHA APARTMENT, SARASWATINAGAR, NEAR UDYOG BHAVAN, SANGLI-416416 M 9423829680 O. 0233-2672888
EMAIL: cadeshpandeassociates2006@gmail.com
Website: www.cadeshpandeassociates.com

Solution

Solution type: Mitigation

The configuration of this services should be changed so that it does not accept the listed cipher suites anymore.

Please see the references for more resources supporting you with this task.

Affected Software/OS

Services accepting vulnerable SSL/TLS cipher suites via HTTPS.

Vulnerability Insight

These rules are applied for the evaluation of the vulnerable cipher suites:

- 64-bit block cipher 3DES vulnerable to the SWEET32 attack (CVE-2016-2183).

Vulnerability Detection Method

Details: SSL/TLS: Report Vulnerable Cipher Suites for HTTPS (OID: 1.3.6.1.4.1.25623.1.0.108031)

Version used: 2021-09-20T09:01:50Z

References

CVE:	CVE-2016-2183, CVE-2016-6329, CVE-2020-12872
Other:	https://bettercrypto.org/
	https://mozilla.github.io/server-side-tls/ssl-config-generator/
	https://sweet32.info/
CERT:	CB-K21/1094, CB-K20/1023, CB-K20/0321, CB-K20/0314, CB-K20/0157, CB-K19/0618, CB-K19/0615, CB-K18/0296, CB-K17/1980, CB-K17/1871, CB-K17/1803, CB-K17/1753, CB-K17/1750, CB-K17/1709, CB-K17/1558, CB-K17/1273, CB-K17/1202, CB-K17/1196, CB-K17/1055, CB-K17/1026, CB-K17/0939, CB-K17/0917, CB-K17/0915, CB-K17/0877, CB-K17/0796, CB-K17/0724, CB-K17/0661, CB-K17/0657, CB-K17/0582, CB-K17/0581, CB-K17/0506, CB-K17/0504, CB-K17/0467,

DESHPANDE & ASSOCIATES
CHARTERED ACCOUNTANTS
ADDRESS: FLAT NO 4, MANISHA APARTMENT, SARASWATINAGAR, NEAR UDYOG BHAVAN, SANGLI-416416 M 9423829680 O. 0233-2672888
EMAIL: cadeshpandeassociates2006@gmail.com
Website: www.cadeshpandeassociates.com

	CB-K17/0345, CB-K17/0098, CB-K17/0089, CB-K17/0086, CB-K17/0082, CB-K16/1837, CB-K16/1830, CB-K16/1635, CB-K16/1630, CB-K16/1624, CB-K16/1622, CB-K16/1500, CB-K16/1465, CB-K16/1307, CB-K16/1296, DFN-CERT-2021-1618, DFN-CERT-2021-0775, DFN-CERT-2021-0770, DFN-CERT-2021-0274, DFN-CERT-2020-2141, DFN-CERT-2020-0368, DFN-CERT-2019-1455, DFN-CERT-2019-0068, DFN-CERT-2018-1296, DFN-CERT-2018-0323, DFN-CERT-2017-2070, DFN-CERT-2017-1954, DFN-CERT-2017-1885, DFN-CERT-2017-1831, DFN-CERT-2017-1821, DFN-CERT-2017-1785, DFN-CERT-2017-1626, DFN-CERT-2017-1326, DFN-CERT-2017-1239, DFN-CERT-2017-1238, DFN-CERT-2017-1090, DFN-CERT-2017-1060, DFN-CERT-2017-0968, DFN-CERT-2017-0947, DFN-CERT-2017-0946, DFN-CERT-2017-0904, DFN-CERT-2017-0816, DFN-CERT-2017-0746, DFN-CERT-2017-0677, DFN-CERT-2017-0675, DFN-CERT-2017-0611, DFN-CERT-2017-0609, DFN-CERT-2017-0522, DFN-CERT-2017-0519, DFN-CERT-2017-0482, DFN-CERT-2017-0351, DFN-CERT-2017-0090, DFN-CERT-2017-0089, DFN-CERT-2017-0088, DFN-CERT-2017-0086, DFN-CERT-2016-1943, DFN-CERT-2016-1937, DFN-CERT-2016-1732, DFN-CERT-2016-1726, DFN-CERT-2016-1715, DFN-CERT-2016-1714, DFN-CERT-2016-1588, DFN-CERT-2016-1555, DFN-CERT-2016-1391, DFN-CERT-2016-1378

5. IP Address: 14.139.120.76

Summary

This document reports on the results of an automatic security scan. The report first summarises the results found. Then, for each host, the report describes every issue found. Please consider the advice given in each description, in order to rectify the issue.

This report might not show details of all issues that were found. Issues with the threat level "Debug" are not shown. Issues with the threat level "False Positive" are not shown. Only results with a minimum QoD of 70 are shown.

All dates are displayed using the timezone "Coordinated Universal Time", which is abbreviated "UTC".

Scan started:	Tue Jun 14 17:25:55 2022
Scan ended:	Tue Jun 14 18:10:54 2022
Task:	Scan of 14.139.120.76

DESHPANDE & ASSOCIATES
CHARTERED ACCOUNTANTS
ADDRESS: FLAT NO 4, MANISHA APARTMENT, SARASWATINAGAR, NEAR UDYOG BHAVAN, SANGLI-416416 M 9423829680 O. 0233-2672888
EMAIL: cadeshpandeassociates2006@gmail.com
Website: www.cadeshpandeassociates.com

Host Summary

Host	Start	End	High	Medium	Low	Log	False Positive
14.139.120.76	Jun 14, 17:26:44	Jun 14, 18:10:51	0	2	0	21	0
Total: 0			0	2	0	21	0

Results per Host

Host 14.139.120.76

Scanning of this host started at:	Tue Jun 14 17:26:44 2022
Number of results:	23

Port Summary for Host 14.139.120.76

Service (Port)	Threat Level
general/CPE-T	Log
443/tcp	Medium
general/tcp	Log

Security Issues for Host 14.139.120.76

443/tcp

Medium (CVSS: 4.0)

NVT: SSL/TLS: Certificate Signed Using A Weak Signature Algorithm (OID: 1.3.6.1.4.1.25623.1.0.105880)

Summary

The remote service is using a SSL/TLS certificate in the certificate chain that has been signed using a cryptographically weak hashing algorithm.

Vulnerability Detection Result

DESHPANDE & ASSOCIATES
CHARTERED ACCOUNTANTS
ADDRESS: FLAT NO 4, MANISHA APARTMENT, SARASWATINAGAR, NEAR UDYOG BHAVAN, SANGLI-416416 M 9423829680 O. 0233-2672888
EMAIL: cadeshpandeassociates2006@gmail.com
Website: www.cadeshpandeassociates.com

The following certificates are part of the certificate chain but using insecure signature algorithms:

Subject: CN=192.168.168.168,OU=HTTPS Management Certificate for SonicWALL (self-signed),O=HTTPS Management Certificate for SonicWALL (self-signed),L=Sunnyvale,ST=California,C=US
Signature Algorithm: sha1WithRSAEncryption

Solution

Solution type: Mitigation

Servers that use SSL/TLS certificates signed with a weak SHA-1, MD5, MD4 or MD2 hashing algorithm will need to obtain new SHA-2 signed SSL/TLS certificates to avoid web browser SSL/TLS certificate warnings.

Vulnerability Insight

The following hashing algorithms used for signing SSL/TLS certificates are considered cryptographically weak and not secure enough for ongoing use:

- Secure Hash Algorithm 1 (SHA-1)

- Message Digest 5 (MD5)

- Message Digest 4 (MD4)

- Message Digest 2 (MD2)

Beginning as late as January 2017 and as early as June 2016, browser developers such as Microsoft and Google will begin warning users when visiting web sites that use SHA-1 signed Secure Socket Layer (SSL) certificates.

NOTE: The script preference allows to set one or more custom SHA-1 fingerprints of CA certificates which are trusted by this routine. The fingerprints needs to be passed comma-separated and case-insensitive:

Fingerprint1

DESHPANDE & ASSOCIATES
CHARTERED ACCOUNTANTS
ADDRESS: FLAT NO 4, MANISHA APARTMENT, SARASWATINAGAR, NEAR UDYOG BHAVAN, SANGLI-416416 M 9423829680 O. 0233-2672888
EMAIL: cadeshpandeassociates2006@gmail.com
Website: www.cadeshpandeassociates.com

or

fingerprint1, Fingerprint2

Vulnerability Detection Method

Check which hashing algorithm was used to sign the remote SSL/TLS certificate.

Details: SSL/TLS: Certificate Signed Using A Weak Signature Algorithm (OID: 1.3.6.1.4.1.25623.1.0.105880)

Version used: 2021-10-15T11:13:32Z

References

Other:	https://blog.mozilla.org/security/2014/09/23/phasing-out-certificates-with-sha-1-based-signature-algorithms/

443/tcp

Medium (CVSS: 4.3)

NVT: SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection (OID: 1.3.6.1.4.1.25623.1.0.117274)

Summary

It was possible to detect the usage of the deprecated TLSv1.0 and/or TLSv1.1 protocol on this system.

Vulnerability Detection Result

In addition to TLSv1.2+ the service is also providing the deprecated TLSv1.1 protocol and supports one or more ciphers. Those supported ciphers can be found in the 'SSL/TLS: Report Supported Cipher Suites' (OID: 1.3.6.1.4.1.25623.1.0.802067) VT.

Impact

An attacker might be able to use the known cryptographic flaws to eavesdrop the connection between clients and the service to get access to sensitive data transferred within the secured connection.

DESHPANDE & ASSOCIATES
CHARTERED ACCOUNTANTS
ADDRESS: FLAT NO 4, MANISHA APARTMENT, SARASWATINAGAR, NEAR UDYOG BHAVAN, SANGLI-416416 M 9423829680 O. 0233-2672888
EMAIL: cadeshpandeassociates2006@gmail.com
Website: www.cadeshpandeassociates.com

	https://datatracker.ietf.org/doc/rfc8996/
	https://vnhacker.blogspot.com/2011/09/beast.html
	https://web.archive.org/web/20201108095603/https://censys.io/blog/freak
	https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters-report-2014
CERT:	CB-K18/0799, CB-K16/1289, CB-K16/1096, CB-K15/1751, CB-K15/1266, CB-K15/0850, CB-K15/0764, CB-K15/0720, CB-K15/0548, CB-K15/0526, CB-K15/0509, CB-K15/0493, CB-K15/0384, CB-K15/0365, CB-K15/0364, CB-K15/0302, CB-K15/0192, CB-K15/0079, CB-K15/0016, CB-K14/1342, CB-K14/0231, CB-K13/0845, CB-K13/0796, CB-K13/0790, DFN-CERT-2020-0177, DFN-CERT-2020-0111, DFN-CERT-2019-0068, DFN-CERT-2018-1441, DFN-CERT-2018-1408, DFN-CERT-2016-1372, DFN-CERT-2016-1164, DFN-CERT-2016-0388, DFN-CERT-2015-1853, DFN-CERT-2015-1332, DFN-CERT-2015-0884, DFN-CERT-2015-0800, DFN-CERT-2015-0758, DFN-CERT-2015-0567, DFN-CERT-2015-0544, DFN-CERT-2015-0530, DFN-CERT-2015-0396, DFN-CERT-2015-0375, DFN-CERT-2015-0374, DFN-CERT-2015-0305, DFN-CERT-2015-0199, DFN-CERT-2015-0079, DFN-CERT-2015-0021, DFN-CERT-2014-1414, DFN-CERT-2013-1847, DFN-CERT-2013-1792, DFN-CERT-2012-1979, DFN-CERT-2012-1829, DFN-CERT-2012-1530, DFN-CERT-2012-1380, DFN-CERT-2012-1377, DFN-CERT-2012-1292, DFN-CERT-2012-1214, DFN-CERT-2012-1213, DFN-CERT-2012-1180, DFN-CERT-2012-1156, DFN-CERT-2012-1155, DFN-CERT-2012-1039, DFN-CERT-2012-0956, DFN-CERT-2012-0908, DFN-CERT-2012-0868, DFN-CERT-2012-0867, DFN-CERT-2012-0848, DFN-CERT-2012-0838, DFN-CERT-2012-0776, DFN-CERT-2012-0722, DFN-CERT-2012-0638, DFN-CERT-2012-0627, DFN-CERT-2012-0451, DFN-CERT-2012-0418, DFN-CERT-2012-0354, DFN-CERT-2012-0234, DFN-CERT-2012-0221, DFN-CERT-2012-0177, DFN-CERT-2012-0170, DFN-CERT-2012-0146, DFN-CERT-2012-0142, DFN-CERT-2012-0126, DFN-CERT-2012-0123, DFN-CERT-2012-0095, DFN-CERT-2012-0051, DFN-CERT-2012-0047, DFN-CERT-2012-0021, DFN-CERT-2011-1953, DFN-CERT-2011-1946, DFN-CERT-2011-1844, DFN-CERT-2011-1826, DFN-CERT-2011-1774, DFN-CERT-2011-1743, DFN-CERT-2011-1738, DFN-CERT-2011-1706, DFN-CERT-2011-1628, DFN-CERT-2011-1627, DFN-CERT-2011-1619, DFN-CERT-2011-1482