VULNERABILITY REPORT

1. *SSL/TLS: Report Weak Cipher Suites* **Severity 5.9 (Medium)**

- *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.

- *IMPACT* - The acceptance of weak SSL/TLS cipher suites in the service poses a medium-severity security risk, potentially leading to unauthorized data exposure, man-in-the-middle attacks, cryptographic weaknesses, and regulatory compliance issues, and the suggested mitigation involves modifying the service configuration to disallow the use of the reported weak cipher suites.

- *SOLUTION* - Solution Type: ⇔ Mitigation

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

2. *SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection* **Severity 5.9 (Medium)**

- *SUMMARY* - It was possible to detect the usage of the deprecated SSLv2 and/or SSLv3 protocol on this system.

- *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 SSLv2 and/or SSLv3 protocols in favor of the TLSv1.2+ protocols. Please see the references for more information.

3. *SSL/TLS: Server Certificate / Certificate in Chain with RSA keys less than 2048 bits* **Severity 5.3 (Medium)**

- *SUMMARY* - It was possible to detect the usage of the deprecated SSLv2 and/or SSLv3 protocol on this system.

- *IMPACT* - Using certificates with weak RSA key size can lead to unauthorized exposure of sensitive information.

- *SOLUTION* - Solution Type: ⇔ Mitigation

- Replace the certificate with a stronger key and reissue the certificates it signed.

4. *Weak (Small) Public Key Size(s) (SSH)* **Severity 5.3 (Medium)**

- *SUMMARY* - The remote SSH server uses a weak (too small) public key size.

- *IMPACT* - A man-in-the-middle attacker can exploit this vulnerability to record the communication to decrypt the session key and even the messages.

- *SOLUTION* - Solution Type: ⇔ Mitigation

- ⇐ 1024 bit for RSA based keys:

- Install a RSA public key length of 2048 bits or greater, or to switch to more secure key types.

5. *SSL/TLS: Server Certificate / Certificate in Chain with RSA keys less than 1024 bits* **Severity 5.3 (Medium)**

- *SUMMARY* - The remote SSL/TLS server certificate and/or any of the certificates in the certificate chain is using a RSA key with less than 1024 bits.

- *IMPACT* - sing certificates with weak RSA key size can lead to unauthorized exposure of sensitive information.

- *SOLUTION* - Solution Type: ⇔ Mitigation

- Replace the certificate with a stronger key and reissue the certificates it signed.

6. *Weak Key Exchange (KEX) Algorithm(s) Supported (SSH)* **Severity 5.3 (Medium)**

- *SUMMARY* - The remote SSH server is configured to allow / support weak key exchange (KEX) algorithm(s).

- *IMPACT* - An attacker can quickly break individual connections.

- *SOLUTION* - Solution Type: ⇔ Mitigation

- Disable the reported weak KEX algorithm(s)

- 1024-bit MODP group / prime KEX algorithms:

Alternatively use elliptic-curve Diffie-Hellmann in general, e.g. Curve 25519..

7. *SSL/TLS: Report 'Null' Cipher Suites* **Severity 5.0 (Medium)**

- *SUMMARY* - It was possible to detect the usage of the deprecated SSLv2 and/or SSLv3 protocol on this system.

- *IMPACT* - This could allow remote attackers to obtain sensitive information or have other, unspecified impacts.

- *SOLUTION* - Solution Type: ⇔ Mitigation

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

8. *SSL/TLS: RSA Temporary Key Handling 'RSA_EXPORT' Downgrade Issue (FREAK)* **Severity 4.3 (Medium)**

- *SUMMARY* - This host is accepting 'RSA_EXPORT' cipher suites and is prone to man in the middle attack.

- *IMPACT* - Successful exploitation will allow remote attacker to downgrade the security of a session to use 'RSA_EXPORT' cipher suites, which are significantly weaker than non-export cipher suites. This may allow a man-in-the-middle attacker to more easily break the encryption and monitor or tamper with the encrypted stream.

- *SOLUTION* - Solution Type: 🔨 Vendorfix

- Remove support for 'RSA_EXPORT' cipher suites from the service.

- If running OpenSSL update to version 0.9.8zd or 1.0.0p or 1.0.1k or later.

9. *Weak Encryption Algorithm(s) Supported (SSH)* **Severity 4.3 (Medium)**

- *SUMMARY* - The remote SSH server is configured to allow / support weak encryption algorithm(s).

- *IMPACT* - The medium-severity risk of the remote SSH server allowing weak encryption algorithms includes heightened vulnerability to attacks, potential unauthorized access, and a concern that newly discovered vulnerabilities may not receive updates, with the recommended solution being to disable the weak encryption algorithm(s).

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

- *SOLUTION* - Solution Type: ⇔ Mitigation

- Disable the reported weak encryption algorithm(s).

10. *SSL/TLS: 'DHE_EXPORT" Man in the Middle Security Bypass Vulnerability (LogJam)* **Severity 3.7 (Low)**

- *SUMMARY* - This host is accepting 'DHE_EXPORT' cipher suites and is prone to man in the middle attack.

- *IMPACT* - Successful exploitation will allow a man-in-the-middle attacker to downgrade the security of a TLS session to 512-bit export-grade cryptography, which is significantly weaker, allowing the attacker to more easily break the encryption and monitor or tamper with the encrypted stream.

- *SOLUTION* - Solution Type: 🔨 Vendorfix

- Remove support for 'DHE_EXPORT' cipher suites from the service

- If running OpenSSL updateto version 1.0.2b or 1.0.1n or later.

11. *SSL/TLS: SSLv3 Protocol CBC Cipher Suites Information Disclosure Vulnerability (POODLE)* **Severity 3.4 (Low)**

- *SUMMARY* - This host is prone to an information disclosure vulnerability.

- *IMPACT* - Successful exploitation will allow a man-in-the-middle attackers gain access to the plain text data stream.

- *SOLUTION* - Solution Type: ⇔ Mitigation

Possible Mitigations are:

- Disable SSLv3

- Disable cipher suites supporting CBC cipher modes

- Enable TLS_FALLBACK_SCSV if the service is providing TLSv1.0+

12. *TCP Timestamps Information Disclosure* **Severity 2.6 (Low)**

- *SUMMARY* - The remote host implements TCP timestamps and therefore allows to compute the uptime.

- *IMPACT* - A side effect of this feature is that the uptime of the remote host can sometimes be computed.

- *SOLUTION* - Solution Type: ⇔ Mitigation

- To disable TCP timestamps on linux add the line 'net.ipv4.tcp_timestamps = 0' to /etc/sysctl.conf. Execute 'sysctl -p' to apply the settings at runtime.

- To disable TCP timestamps on Windows execute 'netsh int tcp set global timestamps=disabled'

- Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled.

The default behavior of the TCP/IP stack on this Systems is to not use the Timestamp options when initiating TCP connections, but use them if the TCP peer that is initiating communication includes them in their synchronize (SYN) segment.

13. *Weak MAC Algorithm(s) Supported (SSH)* **Severity 2.6 (Low)**

- *SUMMARY* - The remote SSH server is configured to allow / support weak MAC algorithm(s).

- *IMPACT* - The low-severity risk of the remote SSH server allowing weak MAC algorithms involves a potential compromise of data integrity, creating a vulnerability for unauthorized access or communication manipulation.

- *SOLUTION* - Solution Type: ⇔ Mitigation

- Disable the reported weak MAC algorithm(s).