**Vulnerability assessment results**

SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection

**Severity** - medium

**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 these protocols won't receive security updates anymore.

**Solution** - 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.

Weak Key Exchange (KEX) Algorithm(s) Supported (SSH)

**Severity** - medium

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

**Solution** - 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.

SSL/TLS: Server Certificate / Certificate in Chain with RSA keys less than 2048 bits

**Severity** - medium

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

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

SSL/TLS: Server Certificate / Certificate in Chain with RSA keys less than 1024 bits

**Severity** - medium

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

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

Weak (Small) Public Key Size(s) (SSH)

**Severity** - medium

**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** - - <= 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.

SSL/TLS: Report 'Null' Cipher Suites

**Severity** - medium

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

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

SSL/TLS: Report Weak Cipher Suites

**Severity** - medium

**Impact** - N/A

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

SSL/TLS: RSA Temporary Key Handling 'RSA\_EXPORT' Downgrade Issue (FREAK)

**Severity** - medium

**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** - 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.

Weak Encryption Algorithm(s) Supported (SSH)

**Severity** - medium

**Impact** - N/A

**Solution** - Disable the reported weak encryption algorithm(s).

SSL/TLS: 'DHE\_EXPORT' Man in the Middle Security Bypass Vulnerability (LogJam)

**Severity** - Low

**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** - Remove support for 'DHE\_EXPORT' cipher suites from the service If running OpenSSL update to version 1.0.2b or 1.0.1n or later.