SSA-412672: Multiple OpenSSL and OpenSSH Vulnerabilities in SCALANCE X-200RNA Switch Devices before V3.2.7

Publication Date: 2022-12-13
Last Update: 2022-12-13
Current Version: V1.0
CVSS v3.1 Base Score: 9.8

SUMMARY

SCALANCE X-200RNA switch devices before V3.2.7 contain multiple OpenSSL and OpenSSH vulnerabilities. The most severe of these vulnerabilities could allow a denial of service condition or could lead to execution of arbitrary code.

Siemens has released updates for the affected products and recommends to update to the latest versions.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SCALANCE X204RNA (HSR) (6GK5204-0BA00-2MB2): All versions < V3.2.7	Update to V3.2.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109814809/ See further recommendations from section Workarounds and Mitigations
SCALANCE X204RNA (PRP) (6GK5204-0BA00-2KB2): All versions < V3.2.7	Update to V3.2.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109814809/ See further recommendations from section Workarounds and Mitigations
SCALANCE X204RNA EEC (HSR) (6GK5204-0BS00-2NA3): All versions < V3.2.7	Update to V3.2.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109814809/ See further recommendations from section Workarounds and Mitigations
SCALANCE X204RNA EEC (PRP) (6GK5204-0BS00-3LA3): All versions < V3.2.7	Update to V3.2.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109814809/ See further recommendations from section Workarounds and Mitigations
SCALANCE X204RNA EEC (PRP/HSR) (6GK5204-0BS00-3PA3): All versions < V3.2.7	Update to V3.2.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109814809/ See further recommendations from section Workarounds and Mitigations

WORKAROUNDS AND MITIGATIONS

Siemens has identified the following specific workarounds and mitigations that customers can apply to reduce the risk:

- Restrict access to the affected systems, especially to ports 22/tcp and 443/tcp to trusted IP addresses only
- Deactivate the webserver if not required, and if deactivation is supported by the product

Product-specific remediations or mitigations can be found in the section Affected Products and Solution. Please follow the General Security Recommendations.

GENERAL SECURITY RECOMMENDATIONS

As a general security measure, Siemens strongly recommends to protect network access to devices with appropriate mechanisms. In order to operate the devices in a protected IT environment, Siemens recommends to configure the environment according to Siemens' operational guidelines for Industrial Security (Download: https://www.siemens.com/cert/operational-guidelines-industrial-security), and to follow the recommendations in the product manuals.

Additional information on Industrial Security by Siemens can be found at: https://www.siemens.com/industrialsecurity

PRODUCT DESCRIPTION

The SCALANCE X-204RNA Industrial Ethernet network access points enable the cost-effective connection of non-PRP terminal devices to separate parallel networks, where a high availability is required.

VULNERABILITY CLASSIFICATION

The vulnerability classification has been performed by using the CVSS scoring system in version 3.1 (CVSS v3.1) (https://www.first.org/cvss/). The CVSS environmental score is specific to the customer's environment and will impact the overall CVSS score. The environmental score should therefore be individually defined by the customer to accomplish final scoring.

An additional classification has been performed using the CWE classification, a community-developed list of common software security weaknesses. This serves as a common language and as a baseline for weakness identification, mitigation, and prevention efforts. A detailed list of CWE classes can be found at: https://cwe.mitre.org/.

Vulnerability CVE-2003-0190

OpenSSH-portable (OpenSSH) 3.6.1p1 and earlier with PAM support enabled immediately sends an error message when a user does not exist, which allows remote attackers to determine valid usernames via a timing attack.

CVSS v3.1 Base Score	5.3
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C
CWE	CWE-208: Observable Timing Discrepancy

Vulnerability CVE-2003-1562

sshd in OpenSSH 3.6.1p2 and earlier, when PermitRootLogin is disabled and using PAM keyboard-interactive authentication, does not insert a delay after a root login attempt with the correct password, which makes it easier for remote attackers to use timing differences to determine if the password step of a multi-step authentication is successful, a different vulnerability than CVE-2003-0190.

CVSS v3.1 Base Score	8.1
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-362: Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')

Vulnerability CVE-2014-8176

The dtls1_clear_queues function in ssl/d1_lib.c in OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h frees data structures without considering that application data can arrive between a ChangeCipherSpec message and a Finished message, which allows remote DTLS peers to cause a denial of service (memory corruption and application crash) or possibly have unspecified other impact via unexpected application data.

CVSS v3.1 Base Score	7.3
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C
CWE	CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer

Vulnerability CVE-2015-0207

The dtls1_listen function in d1_lib.c in OpenSSL 1.0.2 before 1.0.2a does not properly isolate the state information of independent data streams, which allows remote attackers to cause a denial of service (application crash) via crafted DTLS traffic, as demonstrated by DTLS 1.0 traffic to a DTLS 1.2 server.

CVSS v3.1 Base Score	5.3
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L/E:P/RL:O/RC:C
CWE	CWE-20: Improper Input Validation

Vulnerability CVE-2015-0208

The ASN.1 signature-verification implementation in the rsa_item_verify function in crypto/rsa/rsa_ameth.c in OpenSSL 1.0.2 before 1.0.2a allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via crafted RSA PSS parameters to an endpoint that uses the certificate-verification feature.

CVSS v3.1 Base Score	5.3
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L/E:P/RL:O/RC:C
CWE	CWE-476: NULL Pointer Dereference

Vulnerability CVE-2015-0209

Use-after-free vulnerability in the d2i_ECPrivateKey function in crypto/ec/ec_asn1.c in OpenSSL before 0.9.8zf, 1.0.0 before 1.0.0r, 1.0.1 before 1.0.1m, and 1.0.2 before 1.0.2a might allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly have unspecified other impact via a malformed Elliptic Curve (EC) private-key file that is improperly handled during import.

CVSS v3.1 Base Score	7.3
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C
CWE	CWE-416: Use After Free

Vulnerability CVE-2015-0285

The ssl3_client_hello function in s3_clnt.c in OpenSSL 1.0.2 before 1.0.2a does not ensure that the PRNG is seeded before proceeding with a handshake, which makes it easier for remote attackers to defeat cryptographic protection mechanisms by sniffing the network and then conducting a brute-force attack.

CVSS v3.1 Base Score	4.3
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C
CWE	CWE-310: Cryptographic Issues

Vulnerability CVE-2015-0286

The ASN1_TYPE_cmp function in crypto/asn1/a_type.c in OpenSSL before 0.9.8zf, 1.0.0 before 1.0.0r, 1.0.1 before 1.0.1m, and 1.0.2 before 1.0.2a does not properly perform boolean-type comparisons, which allows remote attackers to cause a denial of service (invalid read operation and application crash) via a crafted X.509 certificate to an endpoint that uses the certificate-verification feature.

CVSS v3.1 Base Score	5.3
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L/E:P/RL:O/RC:C
CWE	CWE-1024: Comparison of Incompatible Types

Vulnerability CVE-2015-0287

The ASN1_item_ex_d2i function in crypto/asn1/tasn_dec.c in OpenSSL before 0.9.8zf, 1.0.0 before 1.0.0r, 1.0.1 before 1.0.1m, and 1.0.2 before 1.0.2a does not reinitialize CHOICE and ADB data structures, which might allow attackers to cause a denial of service (invalid write operation and memory corruption) by leveraging an application that relies on ASN.1 structure reuse.

CVSS v3.1 Base Score	5.3
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L/E:P/RL:O/RC:C
CWE	CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer

Vulnerability CVE-2015-0288

The X509_to_X509_REQ function in crypto/x509/x509_req.c in OpenSSL before 0.9.8zf, 1.0.0 before 1.0.0r, 1.0.1 before 1.0.1m, and 1.0.2 before 1.0.2a might allow attackers to cause a denial of service (NULL pointer dereference and application crash) via an invalid certificate key.

CVSS v3.1 Base Score	5.3
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L/E:P/RL:O/RC:C
CWE	CWE-476: NULL Pointer Dereference

Vulnerability CVE-2015-0289

The PKCS#7 implementation in OpenSSL before 0.9.8zf, 1.0.0 before 1.0.0r, 1.0.1 before 1.0.1m, and 1.0.2 before 1.0.2a does not properly handle a lack of outer ContentInfo, which allows attackers to cause a denial of service (NULL pointer dereference and application crash) by leveraging an application that processes arbitrary PKCS#7 data and providing malformed data with ASN.1 encoding, related to crypto/pkcs7/pk7_doit.c and crypto/pkcs7/pk7_lib.c.

CVSS v3.1 Base Score	5.3
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L/E:P/RL:O/RC:C
CWE	CWE-476: NULL Pointer Dereference

Vulnerability CVE-2015-0290

The multi-block feature in the ssl3_write_bytes function in s3_pkt.c in OpenSSL 1.0.2 before 1.0.2a on 64-bit x86 platforms with AES NI support does not properly handle certain non-blocking I/O cases, which allows remote attackers to cause a denial of service (pointer corruption and application crash) via unspecified vectors.

CVSS v3.1 Base Score	5.3
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L/E:P/RL:O/RC:C
CWE	CWE-476: NULL Pointer Dereference

Vulnerability CVE-2015-0291

The sigalgs implementation in t1_lib.c in OpenSSL 1.0.2 before 1.0.2a allows remote attackers to cause a denial of service (NULL pointer dereference and daemon crash) by using an invalid signature_algorithms extension in the ClientHello message during a renegotiation.

CVSS v3.1 Base Score	5.3
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L/E:P/RL:O/RC:C
CWE	CWE-476: NULL Pointer Dereference

Vulnerability CVE-2015-0292

Integer underflow in the EVP_DecodeUpdate function in crypto/evp/encode.c in the base64-decoding implementation in OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via crafted base64 data that triggers a buffer overflow.

CVSS v3.1 Base Score	7.3
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C
CWE	CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer

Vulnerability CVE-2015-0293

The SSLv2 implementation in OpenSSL before 0.9.8zf, 1.0.0 before 1.0.0r, 1.0.1 before 1.0.1m, and 1.0.2 before 1.0.2a allows remote attackers to cause a denial of service (s2_lib.c assertion failure and daemon exit) via a crafted CLIENT-MASTER-KEY message.

CVSS v3.1 Base Score	5.3
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L/E:P/RL:O/RC:C
CWE	CWE-20: Improper Input Validation

Vulnerability CVE-2015-1787

The ssl3_get_client_key_exchange function in s3_srvr.c in OpenSSL 1.0.2 before 1.0.2a, when client authentication and an ephemeral Diffie-Hellman ciphersuite are enabled, allows remote attackers to cause a denial of service (daemon crash) via a ClientKeyExchange message with a length of zero.

CVSS v3.1 Base Score	3.7
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L/E:P/RL:O/RC:C
CWE	CWE-20: Improper Input Validation

Vulnerability CVE-2015-1788

The BN_GF2m_mod_inv function in crypto/bn/bn_gf2m.c in OpenSSL before 0.9.8s, 1.0.0 before 1.0.0e, 1.0.1 before 1.0.1n, and 1.0.2 before 1.0.2b does not properly handle ECParameters structures in which the curve is over a malformed binary polynomial field, which allows remote attackers to cause a denial of service (infinite loop) via a session that uses an Elliptic Curve algorithm, as demonstrated by an attack against a server that supports client authentication.

CVSS v3.1 Base Score	5.3
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L/E:P/RL:O/RC:C
CWE	CWE-399: Resource Management Errors

Vulnerability CVE-2015-1789

The X509_cmp_time function in crypto/x509/x509_vfy.c in OpenSSL before 0.9.8zg, 1.0.0 before 1.0.0s, 1.0.1 before 1.0.1n, and 1.0.2 before 1.0.2b allows remote attackers to cause a denial of service (out-of-bounds read and application crash) via a crafted length field in ASN1_TIME data, as demonstrated by an attack against a server that supports client authentication with a custom verification callback.

CVSS v3.1 Base Score	7.5
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C
CWE	CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer

Vulnerability CVE-2015-1790

The PKCS7_dataDecodefunction in crypto/pkcs7/pk7_doit.c in OpenSSL before 0.9.8zg, 1.0.0 before 1.0.0s, 1.0.1 before 1.0.1n, and 1.0.2 before 1.0.2b allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a PKCS#7 blob that uses ASN.1 encoding and lacks inner EncryptedContent data.

CVSS v3.1 Base Score	5.3
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L/E:P/RL:O/RC:C
CWE	CWE-476: NULL Pointer Dereference

Vulnerability CVE-2015-1791

Race condition in the ssl3_get_new_session_ticket function in ssl/s3_clnt.c in OpenSSL before 0.9.8zg, 1.0.0 before 1.0.0s, 1.0.1 before 1.0.1n, and 1.0.2 before 1.0.2b, when used for a multi-threaded client, allows remote attackers to cause a denial of service (double free and application crash) or possibly have unspecified other impact by providing a NewSessionTicket during an attempt to reuse a ticket that had been obtained earlier.

CVSS v3.1 Base Score	7.3
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C
CWE	CWE-362: Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')

Vulnerability CVE-2015-1792

The do_free_upto function in crypto/cms/cms_smime.c in OpenSSL before 0.9.8zg, 1.0.0 before 1.0.0s, 1.0.1 before 1.0.1n, and 1.0.2 before 1.0.2b allows remote attackers to cause a denial of service (infinite loop) via vectors that trigger a NULL value of a BIO data structure, as demonstrated by an unrecognized X.660 OID for a hash function.

CVSS v3.1 Base Score	5.3
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L/E:P/RL:O/RC:C
CWE	CWE-399: Resource Management Errors

Vulnerability CVE-2015-1794

The ssl3_get_key_exchange function in ssl/s3_clnt.c in OpenSSL 1.0.2 before 1.0.2e allows remote servers to cause a denial of service (segmentation fault) via a zero p value in an anonymous Diffie-Hellman (DH) ServerKeyExchange message.

CVSS v3.1 Base Score	5.3
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L/E:P/RL:O/RC:C
CWE	CWE-682: Incorrect Calculation

Vulnerability CVE-2015-3193

The Montgomery squaring implementation in crypto/bn/asm/x86_64-mont5.pl in OpenSSL 1.0.2 before 1.0.2e on the x86_64 platform, as used by the BN_mod_exp function, mishandles carry propagation and produces incorrect output, which makes it easier for remote attackers to obtain sensitive private-key information via an attack against use of a (1) Diffie-Hellman (DH) or (2) Diffie-Hellman Ephemeral (DHE) ciphersuite.

CVSS v3.1 Base Score	7.5
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C
CWE	CWE-200: Exposure of Sensitive Information to an Unauthorized Actor

Vulnerability CVE-2015-3194

crypto/rsa/rsa_ameth.c in OpenSSL 1.0.1 before 1.0.1q and 1.0.2 before 1.0.2e allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via an RSA PSS ASN.1 signature that lacks a mask generation function parameter.

CVSS v3.1 Base Score	7.5
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C
CWE	CWE-476: NULL Pointer Dereference

Vulnerability CVE-2015-3195

The ASN1_TFLG_COMBINE implementation in crypto/asn1/tasn_dec.c in OpenSSL before 0.9.8zh, 1.0.0 before 1.0.0t, 1.0.1 before 1.0.1q, and 1.0.2 before 1.0.2e mishandles errors caused by malformed X509_ATTRIBUTE data, which allows remote attackers to obtain sensitive information from process memory by triggering a decoding failure in a PKCS#7 or CMS application.

CVSS v3.1 Base Score	5.3
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L/E:P/RL:O/RC:C
CWE	CWE-200: Exposure of Sensitive Information to an Unauthorized Actor

Vulnerability CVE-2015-3196

ssl/s3_clnt.c in OpenSSL 1.0.0 before 1.0.0t, 1.0.1 before 1.0.1p, and 1.0.2 before 1.0.2d, when used for a multi-threaded client, writes the PSK identity hint to an incorrect data structure, which allows remote servers to cause a denial of service (race condition and double free) via a crafted ServerKeyExchange message.

CVSS v3.1 Base Score	5.3
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L/E:P/RL:O/RC:C
CWE	CWE-362: Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')

Vulnerability CVE-2015-3197

ssl/s2_srvr.c in OpenSSL 1.0.1 before 1.0.1r and 1.0.2 before 1.0.2f does not prevent use of disabled ciphers, which makes it easier for man-in-the-middle attackers to defeat cryptographic protection mechanisms by performing computations on SSLv2 traffic, related to the get_client_master_key and get_client_hello functions.

CVSS v3.1 Base Score	5.9
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C
CWE	CWE-200: Exposure of Sensitive Information to an Unauthorized Actor

Vulnerability CVE-2015-4000

The TLS protocol 1.2 and earlier, when a DHE_EXPORT ciphersuite is enabled on a server but not on a client, does not properly convey a DHE_EXPORT choice, which allows man-in-the-middle attackers to conduct cipher-downgrade attacks by rewriting a ClientHello with DHE replaced by DHE_EXPORT and then rewriting a ServerHello with DHE_EXPORT replaced by DHE, aka the “Logjam” issue.

CVSS v3.1 Base Score	3.7
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C
CWE	CWE-310: Cryptographic Issues

Vulnerability CVE-2015-5352

The x11_open_helper function in channels.c in ssh in OpenSSH before 6.9, when ForwardX11Trusted mode is not used, lacks a check of the refusal deadline for X connections, which makes it easier for remote attackers to bypass intended access restrictions via a connection outside of the permitted time window.

CVSS v3.1 Base Score	5.3
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C
CWE	CWE-264: Permissions, Privileges, and Access Controls

Vulnerability CVE-2015-5600

The kbdint_next_device function in auth2-chall.c in sshd in OpenSSH through 6.9 does not properly restrict the processing of keyboard-interactive devices within a single connection, which makes it easier for remote attackers to conduct brute-force attacks or cause a denial of service (CPU consumption) via a long and duplicative list in the ssh -oKbdInteractiveDevices option, as demonstrated by a modified client that provides a different password for each pam element on this list.

CVSS v3.1 Base Score	8.2
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:H/E:P/RL:O/RC:C
CWE	CWE-264: Permissions, Privileges, and Access Controls

Vulnerability CVE-2015-6563

The monitor component in sshd in OpenSSH before 7.0 on non-OpenBSD platforms accepts extraneous username data in MONITOR_REQ_PAM_INIT_CTX requests, which allows local users to conduct impersonation attacks by leveraging any SSH login access in conjunction with control of the sshd uid to send a crafted MONITOR_REQ_PWNAM request, related to monitor.c and monitor_wrap.c.

CVSS v3.1 Base Score	2.9
CVSS Vector	CVSS:3.1/AV:L/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C
CWE	CWE-20: Improper Input Validation

Vulnerability CVE-2015-6564

Use-after-free vulnerability in the mm_answer_pam_free_ctx function in monitor.c in sshd in OpenSSH before 7.0 on non-OpenBSD platforms might allow local users to gain privileges by leveraging control of the sshd uid to send an unexpectedly early MONITOR_REQ_PAM_FREE_CTX request.

CVSS v3.1 Base Score	7.4
CVSS Vector	CVSS:3.1/AV:L/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-264: Permissions, Privileges, and Access Controls

Vulnerability CVE-2015-6565

sshd in OpenSSH 6.8 and 6.9 uses world-writable permissions for TTY devices, which allows local users to cause a denial of service (terminal disruption) or possibly have unspecified other impact by writing to a device, as demonstrated by writing an escape sequence.

CVSS v3.1 Base Score	8.4
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-264: Permissions, Privileges, and Access Controls

Vulnerability CVE-2015-8325

The do_setup_env function in session.c in sshd in OpenSSH through 7.2p2, when the UseLogin feature is enabled and PAM is configured to read .pam_environment files in user home directories, allows local users to gain privileges by triggering a crafted environment for the /bin/login program, as demonstrated by an LD_PRELOAD environment variable.

CVSS v3.1 Base Score	7.8
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C
CWE	CWE-264: Permissions, Privileges, and Access Controls

Vulnerability CVE-2016-0701

The DH_check_pub_key function in crypto/dh/dh_check.c in OpenSSL 1.0.2 before 1.0.2f does not ensure that prime numbers are appropriate for Diffie-Hellman (DH) key exchange, which makes it easier for remote attackers to discover a private DH exponent by making multiple handshakes with a peer that chose an inappropriate number, as demonstrated by a number in an X9.42 file.

CVSS v3.1 Base Score	3.7
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C
CWE	CWE-200: Exposure of Sensitive Information to an Unauthorized Actor

Vulnerability CVE-2016-0702

The MOD_EXP_CTIME_COPY_FROM_PREBUF function in crypto/bn/bn_exp.c in OpenSSL 1.0.1 before 1.0.1s and 1.0.2 before 1.0.2g does not properly consider cache-bank access times during modular exponentiation, which makes it easier for local users to discover RSA keys by running a crafted application on the same Intel Sandy Bridge CPU core as a victim and leveraging cache-bank conflicts, aka a “CacheBleed” attack.

CVSS v3.1 Base Score	5.1
CVSS Vector	CVSS:3.1/AV:L/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C
CWE	CWE-200: Exposure of Sensitive Information to an Unauthorized Actor

Vulnerability CVE-2016-0703

The get_client_master_key function in s2_srvr.c in the SSLv2 implementation in OpenSSL before 0.9.8zf, 1.0.0 before 1.0.0r, 1.0.1 before 1.0.1m, and 1.0.2 before 1.0.2a accepts a nonzero CLIENT-MASTER-KEY CLEAR-KEY-LENGTH value for an arbitrary cipher, which allows man-in-the-middle attackers to determine the MASTER-KEY value and decrypt TLS ciphertext data by leveraging a Bleichenbacher RSA padding oracle, a related issue to CVE-2016-0800.

CVSS v3.1 Base Score	5.9
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C
CWE	CWE-200: Exposure of Sensitive Information to an Unauthorized Actor

Vulnerability CVE-2016-0704

An oracle protection mechanism in the get_client_master_key function in s2_srvr.c in the SSLv2 implementation in OpenSSL before 0.9.8zf, 1.0.0 before 1.0.0r, 1.0.1 before 1.0.1m, and 1.0.2 before 1.0.2a overwrites incorrect MASTER-KEY bytes during use of export cipher suites, which makes it easier for remote attackers to decrypt TLS ciphertext data by leveraging a Bleichenbacher RSA padding oracle, a related issue to CVE-2016-0800.

CVSS v3.1 Base Score	5.9
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C
CWE	CWE-200: Exposure of Sensitive Information to an Unauthorized Actor

Vulnerability CVE-2016-0705

Double free vulnerability in the dsa_priv_decode function in crypto/dsa/dsa_ameth.c in OpenSSL 1.0.1 before 1.0.1s and 1.0.2 before 1.0.2g allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via a malformed DSA private key.

CVSS v3.1 Base Score	9.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-20: Improper Input Validation

Vulnerability CVE-2016-0777

The resend_bytes function in roaming_common.c in the client in OpenSSH 5.x, 6.x, and 7.x before 7.1p2 allows remote servers to obtain sensitive information from process memory by requesting transmission of an entire buffer, as demonstrated by reading a private key.

CVSS v3.1 Base Score	6.5
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C
CWE	CWE-200: Exposure of Sensitive Information to an Unauthorized Actor

Vulnerability CVE-2016-0778

The (1) roaming_read and (2) roaming_write functions in roaming_common.c in the client in OpenSSH 5.x, 6.x, and 7.x before 7.1p2, when certain proxy and forward options are enabled, do not properly maintain connection file descriptors, which allows remote servers to cause a denial of service (heap-based buffer overflow) or possibly have unspecified other impact by requesting many forwardings.

CVSS v3.1 Base Score	8.1
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer

Vulnerability CVE-2016-0797

Multiple integer overflows in OpenSSL 1.0.1 before 1.0.1s and 1.0.2 before 1.0.2g allow remote attackers to cause a denial of service (heap memory corruption or NULL pointer dereference) or possibly have unspecified other impact via a long digit string that is mishandled by the (1) BN_dec2bn or (2) BN_hex2bn function, related to crypto/bn/bn.h and crypto/bn/bn_print.c.

CVSS v3.1 Base Score	7.5
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C
CWE	CWE-20: Improper Input Validation

Vulnerability CVE-2016-0798

Memory leak in the SRP_VBASE_get_by_user implementation in OpenSSL 1.0.1 before 1.0.1s and 1.0.2 before 1.0.2g allows remote attackers to cause a denial of service (memory consumption) by providing an invalid username in a connection attempt, related to apps/s_server.c and crypto/srp/srp_vfy.c.

CVSS v3.1 Base Score	7.5
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C
CWE	CWE-399: Resource Management Errors

Vulnerability CVE-2016-0799

The fmtstr function in crypto/bio/b_print.c in OpenSSL 1.0.1 before 1.0.1s and 1.0.2 before 1.0.2g improperly calculates string lengths, which allows remote attackers to cause a denial of service (overflow and out-of-bounds read) or possibly have unspecified other impact via a long string, as demonstrated by a large amount of ASN.1 data, a different vulnerability than CVE-2016-2842.

CVSS v3.1 Base Score	9.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer

Vulnerability CVE-2016-0800

A cross-protocol attack was discovered that could allow an attacker to decrypt intercepted TLS sessions by using a server supporting SSLv2 as a Bleichenbacher RSA padding oracle. In order to exploit the vulnerability, the attacker must have network access to the affected devices and must be in a privileged network position.

CVSS v3.1 Base Score	4.0
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:L/I:N/A:N/E:P/RL:O/RC:C
CWE	CWE-787: Out-of-bounds Write

Vulnerability CVE-2016-1907

The ssh_packet_read_poll2 function in packet.c in OpenSSH before 7.1p2 allows remote attackers to cause a denial of service (out-of-bounds read and application crash) via crafted network traffic.

CVSS v3.1 Base Score	5.3
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L/E:P/RL:O/RC:C
CWE	CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer

Vulnerability CVE-2016-1908

The client in OpenSSH before 7.2 mishandles failed cookie generation for untrusted X11 forwarding and relies on the local X11 server for access-control decisions, which allows remote X11 clients to trigger a fallback and obtain trusted X11 forwarding privileges by leveraging configuration issues on this X11 server, as demonstrated by lack of the SECURITY extension on this X11 server.

CVSS v3.1 Base Score	9.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-287: Improper Authentication

Vulnerability CVE-2016-2105

Integer overflow in the EVP_EncodeUpdate function in crypto/evp/encode.c in OpenSSL before 1.0.1t and 1.0.2 before 1.0.2h allows remote attackers to cause a denial of service (heap memory corruption) via a large amount of binary data.

CVSS v3.1 Base Score	7.5
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C
CWE	CWE-190: Integer Overflow or Wraparound

Vulnerability CVE-2016-2106

Integer overflow in the EVP_EncryptUpdate function in crypto/evp/evp_enc.c in OpenSSL before 1.0.1t and 1.0.2 before 1.0.2h allows remote attackers to cause a denial of service (heap memory corruption) via a large amount of data.

CVSS v3.1 Base Score	7.5
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C
CWE	CWE-190: Integer Overflow or Wraparound

Vulnerability CVE-2016-2107

The AES-NI implementation in OpenSSL before 1.0.1t and 1.0.2 before 1.0.2h does not consider memory allocation during a certain padding check, which allows remote attackers to obtain sensitive cleartext information via a padding-oracle attack against an AES CBC session. NOTE: this vulnerability exists because of an incorrect fix for CVE-2013-0169.

CVSS v3.1 Base Score	5.9
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C
CWE	CWE-200: Exposure of Sensitive Information to an Unauthorized Actor

Vulnerability CVE-2016-2108

The ASN.1 implementation in OpenSSL before 1.0.1o and 1.0.2 before 1.0.2c allows remote attackers to execute arbitrary code or cause a denial of service (buffer underflow and memory corruption) via an ANY field in crafted serialized data, aka the “negative zero” issue.

CVSS v3.1 Base Score	9.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer

Vulnerability CVE-2016-2109

The asn1_d2i_read_bio function in crypto/asn1/a_d2i_fp.c in the ASN.1 BIO implementation in OpenSSL before 1.0.1t and 1.0.2 before 1.0.2h allows remote attackers to cause a denial of service (memory consumption) via a short invalid encoding.

CVSS v3.1 Base Score	7.5
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C
CWE	CWE-399: Resource Management Errors

Vulnerability CVE-2016-2176

The X509_NAME_oneline function in crypto/x509/x509_obj.c in OpenSSL before 1.0.1t and 1.0.2 before 1.0.2h allows remote attackers to obtain sensitive information from process stack memory or cause a denial of service (buffer over-read) via crafted EBCDIC ASN.1 data.

CVSS v3.1 Base Score	8.2
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:H/E:P/RL:O/RC:C
CWE	CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer

Vulnerability CVE-2016-2177

OpenSSL through 1.0.2h incorrectly uses pointer arithmetic for heap-buffer boundary checks, which might allow remote attackers to cause a denial of service (integer overflow and application crash) or possibly have unspecified other impact by leveraging unexpected malloc behavior, related to s3_srvr.c, ssl_sess.c, and t1_lib.c.

CVSS v3.1 Base Score	9.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-190: Integer Overflow or Wraparound

Vulnerability CVE-2016-2178

The dsa_sign_setup function in crypto/dsa/dsa_ossl.c in OpenSSL through 1.0.2h does not properly ensure the use of constant-time operations, which makes it easier for local users to discover a DSA private key via a timing side-channel attack.

CVSS v3.1 Base Score	5.5
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C
CWE	CWE-203: Observable Discrepancy

Vulnerability CVE-2016-2179

The DTLS implementation in OpenSSL before 1.1.0 does not properly restrict the lifetime of queue entries associated with unused out-of-order messages, which allows remote attackers to cause a denial of service (memory consumption) by maintaining many crafted DTLS sessions simultaneously, related to d1_lib.c, statem_dtls.c, statem_lib.c, and statem_srvr.c.

CVSS v3.1 Base Score	7.5
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C
CWE	CWE-399: Resource Management Errors

Vulnerability CVE-2016-2180

The TS_OBJ_print_bio function in crypto/ts/ts_lib.c in the X.509 Public Key Infrastructure Time-Stamp Protocol (TSP) implementation in OpenSSL through 1.0.2h allows remote attackers to cause a denial of service (out-of-bounds read and application crash) via a crafted time-stamp file that is mishandled by the “openssl ts” command.

CVSS v3.1 Base Score	7.5
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C
CWE	CWE-125: Out-of-bounds Read

Vulnerability CVE-2016-2181

The Anti-Replay feature in the DTLS implementation in OpenSSL before 1.1.0 mishandles early use of a new epoch number in conjunction with a large sequence number, which allows remote attackers to cause a denial of service (false-positive packet drops) via spoofed DTLS records, related to rec_layer_d1.c and ssl3_record.c.

CVSS v3.1 Base Score	7.5
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C
CWE	CWE-682: Incorrect Calculation

Vulnerability CVE-2016-2182

The BN_bn2dec function in crypto/bn/bn_print.c in OpenSSL before 1.1.0 does not properly validate division results, which allows remote attackers to cause a denial of service (out-of-bounds write and application crash) or possibly have unspecified other impact via unknown vectors.

CVSS v3.1 Base Score	9.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-787: Out-of-bounds Write

Vulnerability CVE-2016-2183

The DES and Triple DES ciphers, as used in the TLS, SSH, and IPSec protocols and other protocols and products, have a birthday bound of approximately four billion blocks, which makes it easier for remote attackers to obtain cleartext data via a birthday attack against a long-duration encrypted session, as demonstrated by an HTTPS session using Triple DES in CBC mode, aka a “Sweet32” attack.

CVSS v3.1 Base Score	7.5
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C
CWE	CWE-200: Exposure of Sensitive Information to an Unauthorized Actor

Vulnerability CVE-2016-6210

sshd in OpenSSH before 7.3, when SHA256 or SHA512 are used for user password hashing, uses BLOWFISH hashing on a static password when the username does not exist, which allows remote attackers to enumerate users by leveraging the timing difference between responses when a large password is provided.

CVSS v3.1 Base Score	5.9
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C
CWE	CWE-200: Exposure of Sensitive Information to an Unauthorized Actor

Vulnerability CVE-2016-6302

The tls_decrypt_ticket function in ssl/t1_lib.c in OpenSSL before 1.1.0 does not consider the HMAC size during validation of the ticket length, which allows remote attackers to cause a denial of service via a ticket that is too short.

CVSS v3.1 Base Score	7.5
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C
CWE	CWE-20: Improper Input Validation

Vulnerability CVE-2016-6303

Integer overflow in the MDC2_Update function in crypto/mdc2/mdc2dgst.c in OpenSSL before 1.1.0 allows remote attackers to cause a denial of service (out-of-bounds write and application crash) or possibly have unspecified other impact via unknown vectors.

CVSS v3.1 Base Score	9.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-787: Out-of-bounds Write

Vulnerability CVE-2016-6304

Multiple memory leaks in t1_lib.c in OpenSSL before 1.0.1u, 1.0.2 before 1.0.2i, and 1.1.0 before 1.1.0a allow remote attackers to cause a denial of service (memory consumption) via large OCSP Status Request extensions.

CVSS v3.1 Base Score	7.5
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C
CWE	CWE-401: Missing Release of Memory after Effective Lifetime

Vulnerability CVE-2016-6305

The ssl3_read_bytes function in record/rec_layer_s3.c in OpenSSL 1.1.0 before 1.1.0a allows remote attackers to cause a denial of service (infinite loop) by triggering a zero-length record in an SSL_peek call.

CVSS v3.1 Base Score	7.5
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C
CWE	CWE-20: Improper Input Validation

Vulnerability CVE-2016-6306

The certificate parser in OpenSSL before 1.0.1u and 1.0.2 before 1.0.2i might allow remote attackers to cause a denial of service (out-of-bounds read) via crafted certificate operations, related to s3_clnt.c and s3_srvr.c.

CVSS v3.1 Base Score	5.9
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C
CWE	CWE-125: Out-of-bounds Read

Vulnerability CVE-2016-6307

The state-machine implementation in OpenSSL 1.1.0 before 1.1.0a allocates memory before checking for an excessive length, which might allow remote attackers to cause a denial of service (memory consumption) via crafted TLS messages, related to statem/statem.c and statem/statem_lib.c.

CVSS v3.1 Base Score	5.9
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C
CWE	CWE-400: Uncontrolled Resource Consumption

Vulnerability CVE-2016-6308

statem/statem_dtls.c in the DTLS implementation in OpenSSL 1.1.0 before 1.1.0a allocates memory before checking for an excessive length, which might allow remote attackers to cause a denial of service (memory consumption) via crafted DTLS messages.

CVSS v3.1 Base Score	5.9
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C
CWE	CWE-399: Resource Management Errors

Vulnerability CVE-2016-6515

The auth_password function in auth-passwd.c in sshd in OpenSSH before 7.3 does not limit password lengths for password authentication, which allows remote attackers to cause a denial of service (crypt CPU consumption) via a long string.

CVSS v3.1 Base Score	7.5
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C
CWE	CWE-20: Improper Input Validation

Vulnerability CVE-2016-8858

DISPUTED The kex_input_kexinit function in kex.c in OpenSSH 6.x and 7.x through 7.3 allows remote attackers to cause a denial of service (memory consumption) by sending many duplicate KEXINIT requests. NOTE: a third party reports that “OpenSSH upstream does not consider this as a security issue.”

CVSS v3.1 Base Score	7.5
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C
CWE	CWE-399: Resource Management Errors

Vulnerability CVE-2016-10009

Untrusted search path vulnerability in ssh-agent.c in ssh-agent in OpenSSH before 7.4 allows remote attackers to execute arbitrary local PKCS#11 modules by leveraging control over a forwarded agent-socket.

CVSS v3.1 Base Score	7.3
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L/E:U/RL:O/RC:C
CWE	CWE-426: Untrusted Search Path

Vulnerability CVE-2016-10010

sshd in OpenSSH before 7.4, when privilege separation is not used, creates forwarded Unix-domain sockets as root, which might allow local users to gain privileges via unspecified vectors, related to serverloop.c.

CVSS v3.1 Base Score	7.0
CVSS Vector	CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C
CWE	CWE-264: Permissions, Privileges, and Access Controls

Vulnerability CVE-2016-10011

authfile.c in sshd in OpenSSH before 7.4 does not properly consider the effects of realloc on buffer contents, which might allow local users to obtain sensitive private-key information by leveraging access to a privilege-separated child process.

CVSS v3.1 Base Score	5.5
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:U/RL:O/RC:C
CWE	CWE-264: Permissions, Privileges, and Access Controls

Vulnerability CVE-2016-10012

The shared memory manager (associated with pre-authentication compression) in sshd in OpenSSH before 7.4 does not ensure that a bounds check is enforced by all compilers, which might allows local users to gain privileges by leveraging access to a sandboxed privilege-separation process, related to the m_zback and m_zlib data structures.

CVSS v3.1 Base Score	7.8
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C
CWE	CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer

Vulnerability CVE-2017-3735

While parsing an IPAddressFamily extension in an X.509 certificate, it is possible to do a one-byte overread. This would result in an incorrect text display of the certificate. This bug has been present since 2006 and is present in all versions of OpenSSL before 1.0.2m and 1.1.0g.

CVSS v3.1 Base Score	5.3
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C
CWE	CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer

Vulnerability CVE-2017-15906

The process_open function in sftp-server.c in OpenSSH before 7.6 does not properly prevent write operations in readonly mode, which allows attackers to create zero-length files.

CVSS v3.1 Base Score	5.3
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N/E:U/RL:O/RC:C
CWE	CWE-732: Incorrect Permission Assignment for Critical Resource

Vulnerability CVE-2018-15473

OpenSSH through 7.7 is prone to a user enumeration vulnerability due to not delaying bailout for an invalid authenticating user until after the packet containing the request has been fully parsed, related to auth2-gss.c, auth2-hostbased.c, and auth2-pubkey.c.

CVSS v3.1 Base Score	5.3
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:U/RL:O/RC:C
CWE	CWE-362: Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')

Vulnerability CVE-2018-20685

In OpenSSH 7.9, scp.c in the scp client allows remote SSH servers to bypass intended access restrictions via the filename of . or an empty filename. The impact is modifying the permissions of the target directory on the client side.

CVSS v3.1 Base Score	5.3
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C
CWE	CWE-863: Incorrect Authorization

Vulnerability CVE-2019-1552

OpenSSL has internal defaults for a directory tree where it can find a configuration file as well as certificates used for verification in TLS. This directory is most commonly referred to as OPENSSLDIR, and is configurable with the –prefix / –openssldir configuration options. For OpenSSL versions 1.1.0 and 1.1.1, the mingw configuration targets assume that resulting programs and libraries are installed in a Unix-like environment and the default prefix for program installation as well as for OPENSSLDIR should be '/usr/local'. However, mingw programs are Windows programs, and as such, find themselves looking at sub-directories of 'C:/usr/local', which may be world writable, which enables untrusted users to modify OpenSSL's default configuration, insert CA certificates, modify (or even replace) existing engine modules, etc. For OpenSSL 1.0.2, '/usr/local/ssl' is used as default for OPENSSLDIR on all Unix and Windows targets, including Visual C builds. However, some build instructions for the diverse Windows targets on 1.0.2 encourage you to specify your own –prefix. OpenSSL versions 1.1.1, 1.1.0 and 1.0.2 are affected by this issue. Due to the limited scope of affected deployments this has been assessed as low severity and therefore we are not creating new releases at this time. Fixed in OpenSSL 1.1.1d (Affected 1.1.1-1.1.1c). Fixed in OpenSSL 1.1.0l (Affected 1.1.0-1.1.0k). Fixed in OpenSSL 1.0.2t (Affected 1.0.2-1.0.2s).

CVSS v3.1 Base Score	3.3
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C
CWE	CWE-295: Improper Certificate Validation

Vulnerability CVE-2019-6109

An issue was discovered in OpenSSH 7.9. Due to missing character encoding in the progress display, a malicious server (or Man-in-The-Middle attacker) can employ crafted object names to manipulate the client output, e.g., by using ANSI control codes to hide additional files being transferred. This affects refresh_progress_meter() in progressmeter.c.

CVSS v3.1 Base Score	6.8
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C
CWE	CWE-116: Improper Encoding or Escaping of Output

Vulnerability CVE-2019-6110

In OpenSSH 7.9, due to accepting and displaying arbitrary stderr output from the server, a malicious server (or Man-in-The-Middle attacker) can manipulate the client output, for example to use ANSI control codes to hide additional files being transferred.

CVSS v3.1 Base Score	6.8
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C
CWE	CWE-838: Inappropriate Encoding for Output Context

Vulnerability CVE-2019-6111

An issue was discovered in OpenSSH 7.9. Due to the scp implementation being derived from 1983 rcp, the server chooses which files/directories are sent to the client. However, the scp client only performs cursory validation of the object name returned (only directory traversal attacks are prevented). A malicious scp server (or Man-in-The-Middle attacker) can overwrite arbitrary files in the scp client target directory. If recursive operation (-r) is performed, the server can manipulate subdirectories as well (for example, to overwrite the .ssh/authorized_keys file).

CVSS v3.1 Base Score	5.9
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C
CWE	CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')

Vulnerability CVE-2019-16905

OpenSSH 7.7 through 7.9 and 8.x before 8.1, when compiled with an experimental key type, has a pre-authentication integer overflow if a client or server is configured to use a crafted XMSS key. This leads to memory corruption and local code execution because of an error in the XMSS key parsing algorithm. NOTE: the XMSS implementation is considered experimental in all released OpenSSH versions, and there is no supported way to enable it when building portable OpenSSH.

CVSS v3.1 Base Score	7.8
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-190: Integer Overflow or Wraparound

ADDITIONAL INFORMATION

For further inquiries on security vulnerabilities in Siemens products and solutions, please contact the Siemens ProductCERT:

https://www.siemens.com/cert/advisories

HISTORY DATA

V1.0 (2022-12-13):	Publication Date

TERMS OF USE

Siemens Security Advisories are subject to the terms and conditions contained in Siemens' underlying license terms or other applicable agreements previously agreed to with Siemens (hereinafter "License Terms"). To the extent applicable to information, software or documentation made available in or through a Siemens Security Advisory, the Terms of Use of Siemens' Global Website (https://www.siemens.com/terms_of_use, hereinafter "Terms of Use"), in particular Sections 8-10 of the Terms of Use, shall apply additionally. In case of conflicts, the License Terms shall prevail over the Terms of Use.