THUNDER – IPMI/LOM VULNERABILITIES

PUBLISHED: NOVEMBER 27, 2018 | LAST UPDATE: MAY 2, 2019

SUMMARY

Vulnerability scans of A10 Thunder platform IPMI/LOM (Intelligent Platform Management Interface/Lights Out Management)-interfaces indicated number of vulnerabilities, weaknesses, and unnecessary services; the later of which could cause such scanners to report distracting items of no security consequence or exposure. Accordingly, the following vulnerabilities and scanner-related considerations are addressed in this document.

Item		Score		
#	Vulnerability ID	Source	Score	Summary
1	62565	Nessus	4.3 Med	Transport Layer Security (TLS) Protocol CRIME Vulnerability (CVE-2012-4929) (A)
2	CVE-2012-4929i	cvss2.0	2.6 Low	SSL/TLS CRIME attack against HTTPS (A)
3	62563	Nessus	Info	SSL Compression Methods Supported (A)
4	90317	cvss 2.0	4.3 Med	SSH Weak Algorithms Supported (L)
5	70658	cvss 2.0	2.6 Low	SSH Server CBC Mode Ciphers Enabled (CVE-2008-5161) (A)
6	CVE-2008-5161i	cvss2.0	2.6 Low	OpenSSH: Plaintext Recovery Attack against CBC ciphers (A)
7	71049	cvss 2.0	2.6 Low	SSH Weak MAC Algorithms (A)
8	10267	Nessus	Info	SSH Server Type and Version Information (A)
9	10881	Nessus	Info	SSH Protocol Versions Supported (A)
10	70657	Nessus	Info	SSH Algorithms and Languages Supported (A)
11	39520	Nessus	Info	Backported Security Patch Detection (SSH) (A)
12	10107	Nessus	Info	HTTP Server Type and Version (L)
13	10386	Nessus	Info	Web Server No 404 Error Code Check (A)
14	45590	Nessus	Info	Common Platform Enumeration (CPE) (A)
15	84502	Nessus	Info	HSTS Missing From HTTPS Server (A)
16	42873	cvss 2.0	5.3 Med	SSL Medium Strength Cipher Suites Supported (A, L)
17	94437	cvss 3.0	7.5 High	SSL 64-bit Block Size Cipher Suites Supported (SWEET32) (A, L)
18	CVE-2016-2183i	cvss 3.0	7.5 High	SSL/TLS: Birthday attack against 64-bit block ciphers (SWEET32) (A, L)
19	10114	Nessus	Info	ICMP Timestamp Request Remote Date Disclosure (CVE-1999-0524) (A, L)
20	CVE-1999-0524i	cvss 2.0	0.0 Low	ICMP timestamp response (A, L)
21	11219	Nessus	Info	Nessus SYN scanner (A, L)
22	11936	Nessus	Info	OS Identification (A)
23	22964	Nessus	Info	Service Detection (A)
24	23777	Nessus	Info	SLP Server Detection (TCP) (A, L)
25	23778	Nessus	Info	SLP Server Detection (UDP) (A, L)
26	70544	Nessus	Info	SSL Cipher Block Chaining Cipher Suites Supported (A, L)
27	21643	Nessus	Info	SSL Cipher Suites Supported (A, L)
28	56984	Nessus	Info	SSL / TLS Versions Supported (A, L)
29	68932	Nessus	Info	IPMI Cipher Suites Supported (A, L)
30	72063	Nessus	Info	IPMI Versions Supported (A, L)
31	58751	Nessus	5.3 Med	SSL/TLS Protocol Init Vector Implem Infor Disclosure Vuln (BEAST) (A, L)
32	CVE-2011-3389i	cvss 2.0	4.3 Med	HTTPS: block-wise chosen-plaintext attack against SSL/TLS (BEAST) (A, L)
33	104743	Nessus	Info	TLS Version 1.0 Protocol Detection (A, L)
34	69551	Nessus	Low	SSL Certificate Chain Contains RSA Keys Less Than 2048 bits (A)

(A) Affects Thunder – Group A platforms

(L) Affects Thunder – Group L platforms

AFFECTED RELEASES

Affected A10 Thunder platforms with LOM/IPMI ports that may be exposed to these vulnerabilities are broken down into two groups with the indicated platform models.

Thunder Platform Group	Platforms [a]
Thunder - Group A	• TH1030S • TH3030S, TH3040, TH3230, TH3430 • TH5330
Thunder - Group L	• TH4430, TH4435, TH4440 • TH5430, TH5430-11, TH5430S, TH5435, TH5435S, TH5440, TH5630, TH5840, TH5840-11, TH5845 • TH6430, TH6430S, TH6435, TH6435S, TH6440, TH6630, TH6635 • TH7440, TH7440-11, TH7445 • TH14045-010, TH14045-011

(a) Platforms indicated in the lists above are as of the date of publication for this advisory.
For future A10 Thunder platforms, consult their specifications for presence and support of IPMI/LOM to determine potential exposure to this vulnerability.

The table below indicates versions of Thunder IPMI/LOM firmware exposed to this vulnerability and versions that address it.

Versions Affected	Versions Resolved or Unaffected
Group A – IPMI/LOM FW 3.4.x and prior	3.5.3
Group L – IPMI/LOM FW r1.8 and prior	r1.9e

The version IPMI/LOM firmware supported on a given A10 Thunder system may be determined from the *Device Information* section of the LOM GUI's Dashboard screen, as described in the *A10 Thunder Series and AX Series - Lights Out Management Reference document*.

WORKAROUNDS AND MITIGATIONS

None

SOFTWARE UPDATES

Software, and in this case Firmware, updates that address these vulnerabilities are or will be published at the following URL under the *THUNDER LOM FIRMWARE* heading.

http://www.a10networks.com/support/axseries/software-downloads

For instructions on upgrading the IPMI/LOM firmware in A10 Thunder systems refer to the *Maintenance > Firmware Update* section of the *A10 Thunder Series and AX Series - Lights Out Management Reference document*.

VULNERABILITY DETAILS

The following table shares brief descriptions for the vulnerabilities addressed in this document.

Vulnerability ID	Description
62565	The remote service has a configuration that may make it vulnerable to the CRIME attack. The remote service has one of two configurations that are known to be required for the CRIME attack : - SSL / TLS compression is enabled. - TLS advertises the SPDY protocol earlier than version 4..
CVE-2012-4929i	The TLS protocol 1.2 and earlier, as used in Mozilla Firefox, Google Chrome, Qt, and other products, can encrypt compressed data without properly obfuscating the length of the unencrypted data, which allows man-in-the-middle attackers to obtain plaintext HTTP headers by observing length differences during a series of guesses in

which a string in an HTTP request potentially matches an unknown string in an HTTP header, aka a "CRIME" attack.

62563 The remote service supports one or more compression methods for SSL connections.

This script detects which compression methods are supported by the remote service for SSL connections.

90317 The remote SSH server is configured to allow weak encryption algorithms or no algorithm at all.

Nessus has detected that the remote SSH server is configured to use the Arcfour stream cipher or no cipher at all. RFC 4253 advises against using Arcfour due to an issue with weak keys.

70658 The SSH server is configured to use Cipher Block Chaining.

The SSH server is configured to support Cipher Block Chaining (CBC) encryption. This may allow an attacker to recover the plaintext message from the ciphertext.

CVE-2008-5161i Error handling in the SSH protocol in (1) SSH Tectia Client and Server and Connector 4.0 through 4.4.11, 5.0 through 5.2.4, and 5.3 through 5.3.8; Client and Server and ConnectSecure 6.0 through 6.0.4; Server for Linux on IBM System z 6.0.4; Server for IBM z/OS 5.5.1 and earlier, 6.0.0, and 6.0.1; and Client 4.0-J through 4.3.3-J and 4.0-K through 4.3.10-K; and (2) OpenSSH 4.7p1 and possibly other versions, when using a block cipher algorithm in Cipher Block Chaining (CBC) mode, makes it easier for remote attackers to recover certain plaintext data from an arbitrary block of ciphertext in an SSH session via unknown vectors.

71049 The remote SSH server is configured to allow either MD5 or 96-bit MAC algorithms, both of which are considered weak.

Note that this plugin only checks for the options of the SSH server, and it does not check for vulnerable software versions.

10267 An SSH server is listening on this port.

It is possible to obtain information about the remote SSH server by sending an empty authentication request.

10881 A SSH server is running on the remote host.

This plugin determines the versions of the SSH protocol supported by the remote SSH daemon.

70657 An SSH server is listening on this port.

This script detects which algorithms and languages are supported by the remote service for encrypting communications.

39520 Security patches are backported.

Security patches may have been 'backported' to the remote SSH server without changing its version number.

Banner-based checks have been disabled to avoid false positives.

10107 A web server is running on the remote host.

This plugin attempts to determine the type and the version of the remote web server.

10386 The remote web server does not return 404 error codes.

The remote web server is configured such that it does not return '404 Not Found' error codes when a nonexistent file is requested, perhaps returning instead a site map, search page or authentication page.

Nessus has enabled some counter measures for this. However, they might be insufficient. If a great number of security holes are produced for this port, they might not all be accurate.

45590 It was possible to enumerate CPE names that matched on the remote system.

By using information obtained from a Nessus scan, this plugin reports CPE (Common Platform Enumeration) matches for various hardware and software products found on a host.

Note that if an official CPE is not available for the product, this plugin computes the best possible CPE based on the information available from the scan.

84502 The remote HTTPS server is not enforcing HTTP Strict Transport Security (HSTS). The lack of HSTS allows downgrade attacks, SSL-stripping man-in-the-middle attacks, and weakens cookie-hijacking protections.

42873 The remote host supports the use of SSL ciphers that offer medium strength encryption. Nessus regards medium strength as any encryption that uses key lengths at least 64 bits and less than 112 bits, or else that uses the 3DES encryption suite.

Note that it is considerably easier to circumvent medium strength encryption if the attacker is on the same physical network.

See also :
https://www.openssl.org/blog/blog/2016/08/24/sweet32/

94437 The remote host supports the use of a block cipher with 64-bit blocks in one or more cipher suites. It is, therefore, affected by a vulnerability, known as SWEET32, due to the use of weak 64-bit block ciphers. A man-in-the-middle attacker who has sufficient resources can exploit this vulnerability, via a 'birthday' attack, to detect a collision that leaks the XOR between the fixed secret and a known plaintext, allowing the disclosure of the secret text, such as secure HTTPS cookies, and possibly resulting in the hijacking of an authenticated session.

Proof-of-concepts have shown that attackers can recover authentication cookies from an HTTPS session in as little as 30 hours.

Note that the ability to send a large number of requests over the same TLS connection between the client and server is an important requirement for carrying out this attack. If the number of requests allowed for a single connection were limited, this would mitigate the vulnerability. However, Nessus has not checked for such a mitigation.

CVE-2016-2183i 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.

10114 It is possible to determine the exact time set on the remote host.

The remote host answers to an ICMP timestamp request. This allows anattacker to know the date that is set on the targeted machine, which may assist an unauthenticated, remote attacker in defeating time-based authentication protocols.

CVE-1999-0524i ICMP information such as (1) netmask and (2) timestamp is allowed from arbitrary hosts.

11219 This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

11936 It is possible to guess the remote operating system.

Using a combination of remote probes (e.g., TCP/IP, SMB, HTTP, NTP, SNMP, etc.), it is possible to guess the name of the remote operating system in use. It is also possible sometimes to guess the version of the operating system.

22964 The remote service could be identified.

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

23777 The remote server understands Service Location Protocol (SLP), a protocol that allows network applications to discover the existence, location, and configuration of various services in an enterprise network environment. A server that understands SLP can either be a service agent (SA), which knows the location of various services, or a directory agent (DA), which acts as a central repository for service location information.

23778

The remote server understands Service Location Protocol (SLP), a protocol that allows network applications to discover the existence, location, and configuration of various services in an enterprise network environment. A server that understands SLP can either be a service agent (SA), which knows the location of various services, or a directory agent (DA), which acts as a central repository for service location information.

70544

The remote service supports the use of SSL Cipher Block Chaining ciphers, which combine previous blocks with subsequent ones.

The remote host supports the use of SSL ciphers that operate in Cipher Block Chaining (CBC) mode. These cipher suites offer additional security over Electronic Codebook (ECB) mode, but have the potential to leak information if used improperly.

21643

The remote service encrypts communications using SSL.

This plugin detects which SSL ciphers are supported by the remote service for encrypting communications.

56984

The remote service encrypts communications.

This plugin detects which SSL and TLS versions are supported by the remote service for encrypting communications.

68932

The remote service provides cryptographic means of protecting communications.

This script detects which IPMI cipher suites are supported by the remote service for the authentication, integrity, and confidentiality of communications.

72063

The remote service implements a management protocol.

This script detects which IPMI versions are supported by the remote service for managing the system, as well as additional settings.

58751

A vulnerability exists in SSL 3.0 and TLS 1.0 that could allow information disclosure if an attacker intercepts encrypted traffic served from an affected system.

TLS 1.1, TLS 1.2, and all cipher suites that do not use CBC mode are not affected.

This plugin tries to establish an SSL/TLS remote connection using an affected SSL version and cipher suite and then solicits return data. If returned application data is not fragmented with an empty or one-byte record, it is likely vulnerable.

OpenSSL uses empty fragments as a countermeasure unless the 'SSL_OP_DONT_INSERT_EMPTY_FRAGMENTS' option is specified when OpenSSL is initialized.

Note that this plugin detects the vulnerability in the SSLv3/TLSv1 protocol implemented in the server. It does not detect the BEAST attack where it exploits the vulnerability at HTTPS client-side (i.e., Internet browser). The detection at server-side does not necessarily mean your server is vulnerable to the BEAST attack, because the attack exploits the vulnerability at the client-side, and both SSL/TLS clients and servers can independently employ the split record countermeasure.

CVE-2011-3389i

The SSL protocol, as used in certain configurations in Microsoft Windows and Microsoft Internet Explorer, Mozilla Firefox, Google Chrome, Opera, and other products, encrypts data by using CBC mode with chained initialization vectors, which allows man-in-the-middle attackers to obtain plaintext HTTP headers via a blockwise chosen-boundary attack (BCBA) on an HTTPS session, in conjunction with JavaScript code that uses (1) the HTML5 WebSocket API, (2) the Java URLConnection API, or (3) the Silverlight WebClient API, aka a "BEAST" attack.

104743

The remote service accepts connections encrypted using TLS 1.0. TLS 1.0 has a number of cryptographic design flaws. Modern implementations of TLS 1.0 mitigate these problems, but newer versions of TLS like 1.1 and 1.2 are designed against these flaws and should be used whenever possible.

PCI DSS v3.1 requires that TLS 1.0 be disabled entirely by June 2018, except for point-of-sale terminals and their

	termination points.
69551	At least one of the X.509 certificates sent by the remote host has a key that is shorter than 2048 bits. According to industry standards set by the Certification Authority/Browser (CA/B) Forum, certificates issued after January 1, 2014 must be at least 2048 bits. Some browser SSL implementations may reject keys less than 2048 bits after January 1, 2014. Additionally, some SSL certificate vendors may revoke certificates less than 2048 bits before January 1, 2014. Note that Nessus will not flag root certificates with RSA keys less than 2048 bits if they were issued prior to December 31, 2010, as the standard considers them exempt.

RELATED LINKS

Ref #	General Link
[1]	https://www.tenable.com/plugins/index.php?view=single&id=62565
[2]	https://nvd.nist.gov/vuln/detail/CVE-2012-4929
[3]	https://www.tenable.com/plugins/index.php?view=single&id=62563
[4]	https://www.tenable.com/plugins/index.php?view=single&id=90317
[5]	https://www.tenable.com/plugins/index.php?view=single&id=70658
[6]	https://nvd.nist.gov/vuln/detail/CVE-2008-5161
[7]	https://www.tenable.com/plugins/index.php?view=single&id=71049
[8]	https://www.tenable.com/plugins/index.php?view=single&id=10267
[9]	https://www.tenable.com/plugins/index.php?view=single&id=10881
[10]	https://www.tenable.com/plugins/index.php?view=single&id=70657
[11]	https://www.tenable.com/plugins/index.php?view=single&id=39520
[12]	https://www.tenable.com/plugins/index.php?view=single&id=10107
[13]	https://www.tenable.com/plugins/index.php?view=single&id=10386
[14]	https://www.tenable.com/plugins/index.php?view=single&id=45590
[15]	https://www.tenable.com/plugins/index.php?view=single&id=84502
[16]	https://www.tenable.com/plugins/index.php?view=single&id=42873
[17]	https://www.tenable.com/plugins/index.php?view=single&id=94437
[18]	https://nvd.nist.gov/vuln/detail/CVE-2016-2183
[19]	https://www.tenable.com/plugins/index.php?view=single&id=10114
[20]	https://nvd.nist.gov/vuln/detail/CVE-1999-0524
[21]	https://www.tenable.com/plugins/index.php?view=single&id=11219
[22]	https://www.tenable.com/plugins/index.php?view=single&id=11936
[23]	https://www.tenable.com/plugins/index.php?view=single&id=22964
[24]	https://www.tenable.com/plugins/index.php?view=single&id=23777
[25]	https://www.tenable.com/plugins/index.php?view=single&id=23778
[26]	https://www.tenable.com/plugins/index.php?view=single&id=70544
[27]	https://www.tenable.com/plugins/index.php?view=single&id=21643
[28]	https://www.tenable.com/plugins/index.php?view=single&id=56984
[29]	https://www.tenable.com/plugins/index.php?view=single&id=68932
[30]	https://www.tenable.com/plugins/index.php?view=single&id=72063
[31]	https://www.tenable.com/plugins/index.php?view=single&id=58751
[32]	https://nvd.nist.gov/vuln/detail/CVE-2011-3389
[33]	https://www.tenable.com/plugins/index.php?view=single&id=104743
[34]	https://www.tenable.com/plugins/index.php?view=single&id=69551

ACKNOWLEDGEMENTS

None

MODIFICATION HISTORY

Revision	Date	Description
1.0	2018-11-27	Initial Publication
2.0	2019-05-02	Corrected Group L resolved firmware version from r1.9 to r1.9e

This document is provided on an "AS IS" basis and does not imply any kind of guarantee or warranty, including the warranties of merchantability, non-infringement or fitness for a particular use. Your use of the information in this document or materials linked from this document is at your own risk. A10 Networks, Inc. reserves the right to change or update the information in this document at any time.