THUNDER LOM/IPMI - CVE-2013-4786

PUBLISHED: JULY 22, 2018 | LAST UPDATE: JULY 22, 2018

SUMMARY

A vulnerability exists on the Lights-Out Management/Intelligent Platform Management Interface (LOM/IPMI) port of A10 Thunder devices could allow remote attacker to mount an offline, brute-force, guessing attack of the configured password.

This vulnerability is due to support for the RMCP+ Authenticated Key-Exchange (RAKP) Protocol as part of the IPMI Version 2.0 capability provided on the LOM/IPMI port for out-of-band management of Thunder devices. A flaw or limitation in the of RAKP Protocol and the HMAC information in RAKP Message 2 responses exposes password hash information that could be leveraged in such an attack and potentially and gain unauthorized access to out-of-band management services of the device.

A10 Thunder platforms that do not have an LOM/IPMI port are beyond the scope of this advisory and not exposed to this vulnerability.

There is no patch for this vulnerability; it is an inherent problem with specifications for IPMI v2.0.

Item		**Score**		
#	**Vulnerability ID**	**Source**	**Score**	**Summary**
1	CVE-2013-4786	CVSS 3.0	7.5 High	IPMI: Leakage of password hashes via RAKP authentication [1]
2	80101	Nessus	7.8 High	IPMI v2.0 Password Hash Disclosure [2]

AFFECTED PLATFORMS AND RELEASES

Affected A10 Thunder platforms with LOM/IPMI ports that may be exploited by this vulnerability 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 LOM/IPMI to determine potential exposure to this vulnerability.

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

Versions Affected	**Versions Resolved or Unaffected**
Group A – LOM/IPMI FW 3.x.x	None planned [(a)]
Group L – LOM/IPMI FW r1.8x	None planned [(a)]

(a) If versions of IPMI become accepted and available in the industry that correct this vulnerability, A10 will consider them for this matter in the future.

WORKAROUNDS AND MITIGATIONS

Mitigations commonly employed in the industry for this issue include:

- Disable the IPMI/LOM port, if it is not essential or needed
- Employ best practices for passwords in systems and networks.
- Use strong passwords to limit the successfulness of off-line, dictionary attacks.
- Use a separate or isolated management LAN/VLAN for IPMI/LOM port connectivity.
- Use Access Control Lists (ACLs) to limit or restrict access to the IPMI/LOM port

SOFTWARE UPDATES

Software updates that address these vulnerabilities are or will be published at the following URL:

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

VULNERABILITY DETAILS

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

Vulnerability ID	Description
CVE-2013-4786	The IPMI 2.0 specification supports RMCP+ Authenticated Key-Exchange Protocol (RAKP) authentication, which allows remote attackers to obtain password hashes and conduct offline password guessing attacks by obtaining the HMAC from a RAKP message 2 response from a BMC.
80101	Synopsis: The remote host supports IPMI version 2.0. Description: The remote host supports IPMI v2.0. The Intelligent Platform Management Interface (IPMI) protocol is affected by an information disclosure vulnerability due to the support of RMCP+ Authenticated Key-Exchange Protocol (RAKP) authentication. A remote attacker can obtain password hash information for valid user accounts via the HMAC from a RAKP message 2 response from a BMC. See also :http://fish2.com/ipmi/remote-pw-cracking.html Ports: udp/623 - Nessus detected that the remote server has IPMI v2.0 implemented. - Remote unauthenticated users will be able to get password hashes for valid users.

RELATED LINKS

Ref #	General Link
[1]	NIST NVD, CVE-2013-4786
[2]	Nessus: IPMI v2.0 Password Hash Disclosure

ACKNOWLEDGEMENTS

None

MODIFICATION HISTORY

Revision	Date	Description
1.0	2018-07-22	Initial Publication

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.