CVE-2019-0140 –ETHERNET CONTROLLER FIRMWARE (TH-3040)

PUBLISHED: APRIL 24, 2020 | LAST UPDATE: APRIL 24, 2020

SUMMARY

In November 2019, Intel published vulnerabilities affecting Intel 700 Series Ethernet Controllers [1]. For A10 Networks, CVE-2019-0140 [2] may allow an escalation of privilege, denial of service or information disclosure. This vulnerability requires adjacent access to the system to exploit the flaw in the controller firmware.

Item #	Vulnerability ID	Score Source	Score	Summary
1	CVE-2019-0140	CVSS 3.0	8.8 High	Buffer overflow in Intel Ethernet 700 Series firmware, privilege escalation via an adjacent access

AFFECTED RELEASES

This is not a vulnerability in ACOS. Rather, this is a vulnerability in the firmware of Intel 700 Series Ethernet Controllers. A10 Networks TH-3040 devices manufactured before April 2020 may have firmware vulnerable to this issue. See the mitigations procedure below for instructions on updating the Intel ethernet controller firmware in affected TH-3040 devices.

Intel 700 Series controllers may also be used in vThunder or Bare Metal ACOS systems. It is the responsibility of the customer in these cases to ensure that Intel 700 Series ethernet controller firmware is updated as appropriate to ensure that these systems are not exposed to this vulnerability.

WORKAROUNDS AND MITIGATIONS

The following mitigation procedure is recommended for all A10 Networks TH-3040 devices manufactured before April 2020, to upgrade their underlying Intel 700 Series Controller firmware.

First, download the “TH3040-update-cve-2019-0140.upg” file from the A10 Networks support software download site to a local system accessible to the TH-3040 device.

Second, update the ethernet controller firmware for A10 Networks TH-3040 devices by using the “upgrade” command in config mode.

```
ACOS(config)# upgrade hd pri use-mgmt-port scp://user@<ip-address>/home/user/TH3040-update-cve-2019-
0140.upg
Password []?

Do you want to reboot the system after the upgrade?[yes/no]:yes
Expand the upgrade package now ...

Done (0 minutes 1 seconds)
Upgrade ...
Upgrade failed
ACOS(config)(LOADING)#[446354.863762] reboot: Restarting system
```

The command output will indicate that the “Upgrade failed” when updating the firmware even when the firmware update succeeds. This merely indicates the ACOS software of the device was not changed and this is expected to be displayed.

The device will reboot after the upgrade command. This is required and will happen even if a “no” response is given to the question “Do you want to reboot the system after the upgrade?”.

Lastly, verify the results of the firmware update operation by viewing the varlog logging entries. Entries similar to the following will indicate that the firmware was successfully updated, by showing the original version followed by the new updated version.

```
show varlog tail 1000 | inc firmware
Mar 13 03:39:21 localhost axlog: firmware-version: 5.02 0x80002470 0.0.0
Mar 13 03:41:53 localhost axlog: firmware-version: 7.10 0x800077fd 0.0.0
```

Entries similar to the following will indicate that the Intel 700 Series firmware was already sufficiently up to date and not exposed to this vulnerability.

```
Mar 13 04:11:35 localhost axlog: firmware already update to latest 0x800077fd
```

If this upgrade is applied to an A10 Networks device that is not a TH-3040, the command will fail as shown below.

```
Checking integrity of upgrade package ...
Incorrect software for the model
```

SOFTWARE UPDATES

Software updates that address these vulnerabilities are or will be published at the following URL, near the bottom in the "Other Updates and Tools" section with the heading "Thunder 3040 Firmware Security Update for CVE-2019-0140":

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-2019-0140	Buffer overflow in firmware for Intel(R) Ethernet 700 Series Controllers before version 7.0 may allow an unauthenticated user to potentially enable an escalation of privilege via an adjacent access.

RELATED LINKS

Ref #	General Link
[1]	Intel® Ethernet 700 Series Controllers Advisory
[2]	https://nvd.nist.gov/vuln/detail/cve-2019-0140

ACKNOWLEDGEMENTS

None

MODIFICATION HISTORY

Revision	Date	Description
1.0	2020-04-24	Initial Publication