CVE-2022-36382 – ETHERNET CONTROLLER FIRMWARE (TH-3350)

PUBLISHED: MARCH 26, 2024 | LAST UPDATE: MAY 23, 2024

Summary

In February 2023, Intel published vulnerabilities affecting some Intel Ethernet Controllers including the 700 Series [1]. For A10 Networks, CVE-2022-36382 [2] may allow an escalation of privilege, denial of service. This vulnerability requires local access to the system to exploit the flaw in the controller firmware.

Item #	Vulnerability ID	Score Source	Score	Summary
1	CVE-2022-36382	CVSSv3.0	8.8 High	Out-of-bounds write in firmware for some Intel Ethernet Network Controllers and Adapters: E810, 700 Series [1]

Affected Releases

This is not a vulnerability in ACOS. Rather, this is a vulnerability in the firmware of Intel E810 and 700 Series Ethernet Controllers. A10 Networks TH-3350 devices manufactured before October 2024 may have firmware vulnerable to this issue. See the mitigations procedure below for instructions on updating the Intel ethernet controller firmware in affected TH-3350 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 mitigation procedure recommended for all A10 Networks TH-3350 devices manufactured before October 2024 is provided to upgrade their underlying Intel 700 Series Controller firmware.

Please contact A10 Networks Technical Support for the required upgrade package.

The serial number provides an indication of TH3350 systems that have this firmware upgrade done during manufacturing.

TH3350-020 and -02E System revision 10 or newer do not need the Ethernet controller firmware upgrade.
TH3350S-020 System revision 0F or newer do not need the Ethernet controller firmware upgrade
The revision is in the SN. TH33 XX 5********* where XX=Revision

Upgrading the Ethernet controller firmware does not change or affect the ACOS software running on the system.

First, download the “TH3350-update-cve-2022-36382v2.upg” file provided by A10 Networks support to a local system accessible to the TH-3350 device.

Second, update the ethernet controller firmware for A10 Networks TH-3350 devices by using the “upgrade” command in config mode. It is important to answer “no” in response to the question “Do you want to reboot the system after the upgrade?”. This allows the upgrade script to complete and initiate the reboot when ready.

```
ACOS(config)# upgrade hd pri use-mgmt-port scp://user@<ip-address>/home/user/TH3350-update-cve-2022-
36382v2.upg
Password []?

Do you want to reboot the system after the upgrade?[yes/no]:no
Getting upgrade package ...
..
Done (0 minutes 1 seconds)
Decrypt upgrade package ...
..
Done (0 minutes 1 seconds)
Checking integrity of upgrade package ...
Upgrade file integrity checking passed (0 minutes 1 seconds)
Expand the upgrade package now ...
.
Done (0 minutes 2 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 though 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 new updated version.

```
show varlog tail 10000 | include firmware-version
May 21 14:44:20 localhost axlog: Current nvm firmware-version: 7.10 0x8000d8bc 0.0.0 on eth1 is out of date
May 21 14:44:27 localhost axlog: Current nvm firmware-version: 7.10 0x8000d8bc 0.0.0 on eth2 is out of date
May 21 14:44:34 localhost axlog: Current nvm firmware-version: 7.10 0x8000d8bc 0.0.0 on eth3 is out of date
May 21 14:44:41 localhost axlog: Current nvm firmware-version: 7.10 0x8000d8bc 0.0.0 on eth4 is out of date
May 21 14:44:48 localhost axlog: Current nvm firmware-version: 7.10 0x8000d8bc 0.0.0 on eth5 is out of date
May 21 14:44:55 localhost axlog: Current nvm firmware-version: 7.10 0x8000d8bc 0.0.0 on eth6 is out of date
May 21 14:45:02 localhost axlog: Current nvm firmware-version: 7.10 0x8000d8bc 0.0.0 on eth7 is out of date
May 21 14:45:09 localhost axlog: Current nvm firmware-version: 7.10 0x8000d8bc 0.0.0 on eth8 is out of date
May 21 14:48:05 localhost axlog: The new nvm firmware-version: 9.20 0x8000d8bc 0.0.0 for eth1.
May 21 14:48:12 localhost axlog: The new nvm firmware-version: 9.20 0x8000d8bc 0.0.0 for eth2.
May 21 14:48:19 localhost axlog: The new nvm firmware-version: 9.20 0x8000d8bc 0.0.0 for eth3.
May 21 14:48:26 localhost axlog: The new nvm firmware-version: 9.20 0x8000d8bc 0.0.0 for eth4.
May 21 14:48:33 localhost axlog: The new nvm firmware-version: 9.20 0x8000d8bc 0.0.0 for eth5.
May 21 14:48:40 localhost axlog: The new nvm firmware-version: 9.20 0x8000d8bc 0.0.0 for eth6.
May 21 14:48:47 localhost axlog: The new nvm firmware-version: 9.20 0x8000d8bc 0.0.0 for eth7.
May 21 14:48:54 localhost axlog: The new nvm firmware-version: 9.20 0x8000d8bc 0.0.0 for eth8.
May 21 14:48:54 localhost axlog: Updated the nvm firmware-version of all Ethernet interfaces successfully.
```

If this upgrade is applied to an A10 Networks device that has already been upgraded or has the same or newer version, entries similar to the following will indicate that the firmware is up to date.

```
May 21 13:32:01 localhost axlog: Current nvm firmware-version: 9.20 0x8000d8bc 0.0.0 on eth1 is up to date
May 21 13:32:07 localhost axlog: Current nvm firmware-version: 9.20 0x8000d8bc 0.0.0 on eth2 is up to date
May 21 13:32:14 localhost axlog: Current nvm firmware-version: 9.20 0x8000d8bc 0.0.0 on eth3 is up to date
May 21 13:32:21 localhost axlog: Current nvm firmware-version: 9.20 0x8000d8bc 0.0.0 on eth4 is up to date
May 21 13:32:28 localhost axlog: Current nvm firmware-version: 9.20 0x8000d8bc 0.0.0 on eth5 is up to date
May 21 13:32:35 localhost axlog: Current nvm firmware-version: 9.20 0x8000d8bc 0.0.0 on eth6 is up to date
May 21 13:32:42 localhost axlog: Current nvm firmware-version: 9.20 0x8000d8bc 0.0.0 on eth7 is up to date
May 21 13:32:49 localhost axlog: Current nvm firmware-version: 9.20 0x8000d8bc 0.0.0 on eth8 is up to date
May 21 13:32:49 localhost axlog: All Ethernet interfaces are already up to date to nvm firmware-version:
9.20 0x8000d8bc 0.0.0.
```

If this upgrade is applied to an A10 Networks device that is not a TH-3350, the command will fail as shown below.

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

If the update was unsuccessful, there will be entries indicating that the update was not successful. This will show the number of interface devices that were updated, if any. For example:

```
May 21 14:44:20 localhost axlog: Current nvm firmware-version: 9.20 0x8000d8bc 0.0.0 on eth5 is up to date
May 21 14:44:27 localhost axlog: Current nvm firmware-version: 9.20 0x8000d8bc 0.0.0 on eth5 is up to date
May 21 14:44:34 localhost axlog: Current nvm firmware-version: 9.20 0x8000d8bc 0.0.0 on eth5 is up to date
May 21 14:44:41 localhost axlog: Current nvm firmware-version: 9.20 0x8000d8bc 0.0.0 on eth5 is up to date
May 21 14:44:48 localhost axlog: Current nvm firmware-version: 7.10 0x8000d8bc 0.0.0 on eth5 is out of date
May 21 14:44:55 localhost axlog: Current nvm firmware-version: 7.10 0x8000d8bc 0.0.0 on eth6 is out of date
May 21 14:45:02 localhost axlog: Current nvm firmware-version: 7.10 0x8000d8bc 0.0.0 on eth7 is out of date
May 21 14:45:09 localhost axlog: Current nvm firmware-version: 7.10 0x8000d8bc 0.0.0 on eth8 is out of date
May 21 14:45:12 localhost axlog: Pre-update check: 4/8 Ethernet interfaces are up to date.
May 21 14:48:05 localhost axlog: The new nvm firmware-version: 9.20 0x8000d8bc 0.0.0 for eth1.
May 21 14:48:12 localhost axlog: The new nvm firmware-version: 9.20 0x8000d8bc 0.0.0 for eth2.
May 21 14:48:19 localhost axlog: The new nvm firmware-version: 9.20 0x8000d8bc 0.0.0 for eth3.
May 21 14:48:26 localhost axlog: The new nvm firmware-version: 9.20 0x8000d8bc 0.0.0 for eth4.
May 21 14:48:33 localhost axlog: The new nvm firmware-version: 7.10 0x8000d8bc 0.0.0 for eth5.
May 21 14:48:40 localhost axlog: The new nvm firmware-version: 7.10 0x8000d8bc 0.0.0 for eth6.
May 21 14:48:47 localhost axlog: The new nvm firmware-version: 7.10 0x8000d8bc 0.0.0 for eth7.
May 21 14:48:54 localhost axlog: The new nvm firmware-version: 7.10 0x8000d8bc 0.0.0 for eth8.
May 21 14:48:54 localhost axlog: Only updated the nvm firmware-version of 4/8 Ethernet interfaces.
```

It is highly unlikely that the firmware update will fail, but if this occurs, please contact A10 Networks customer support.

Software Updates

Software updates that address these vulnerabilities are or will be published at the link below when they are available.

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-2022-36382	Out-of-bounds write in firmware for some Intel(R) Ethernet Network Controllers and Adapters E810 Series before version 1.7.0.8 and some Intel(R) Ethernet 700 Series Controllers and Adapters before version 9.101 may allow a privileged user to potentially enable denial of service via local access.

Related Links

Ref #	General Link
[1]	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00754.html
[2]	http://nvd.nist.gov/vuln/detail/CVE-2022-36382

Acknowledgements

None

Modification History

Revision	Date	Description

1.0	2024-03-26	Initial Publication
2.0	2024-05-23	Update procedure for updated upgrade package

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.