A10 ACOS GUI FILE ACCESS VULNERABILITY

PUBLISHED: SEPTEMBER 12, 2023 | LAST UPDATE: SEPTEMBER 12, 2023

Summary

A vulnerability in the management Graphical User Interface (GUI) of A10 Networks' Advanced Core Operating System (ACOS) may allow authenticated users to view, export, or delete system files from affected Thunder devices.

The vulnerability requires successful user authentication and access to an affected system's management port or an otherwise configured management interface. The vulnerability is not exposed on the system's data plane, management console, or management Command Line Interface (CLI). Mitigating controls may be implemented to significantly reduce risk associated with this vulnerability and are detailed below.

A10 Networks, additionally, recommends that customers apply software updates or hot fixes indicated in this Security Advisory as soon as practical. Hot fixes may be applied without impact to operational ACOS systems.

A10 Networks has assigned reference ID A10-2023-0006 to this vulnerability which reflects Trend Micro Zero Day Initiative research:

Item #	Vulnerability ID	Score Source	Score	Summary
1	ZDI-CAN-17899	CVSSv3	6.5 Medium	A10 Thunder ADC ShowTechDownloadView Directory Traversal Information Disclosure Vulnerability [1]
2	ZDI-CAN-17905	CVSSv3	8.3 High	A10 Thunder ADC FileMgmtExport Directory Traversal Arbitrary File Read and Deletion Vulnerability [2]

A10 Networks monitors the internet through our Threat Intelligence team and is not aware of malicious use of or attempts to exploit this vulnerability.

Affected Releases

The table below indicates releases of ACOS exposed to this vulnerability and ACOS releases that address them. ACOS release families not indicated below are unaffected by these vulnerabilities.

Customers using affected ACOS releases may apply hotfixes or upgrade directly to a corresponding unaffected release as they become available.

Releases Affected			Releases Resolved or Unaffected	Hot Fix
6.0.0	–	6.0.1	6.0.2	HF-20230006.upg
5.2.1-P1	–	5.2.1-P8	5.2.1-P9	HF-20230006.upg
5.1.0	–	5.2.1	5.2.1-P9	None - Upgrade ACOS
4.1.4-GR1-P6	–	4.1.4-GR1-P12	4.1.4-GR1-P13	HF-20230006.upg
4.1.4	–	4.1.4-GR1-P5	4.1.4-GR1-P13	None - Upgrade ACOS

Workarounds and Mitigations

Disable GUI Management - ACOS

If not required, disabling the GUI management service fully mitigates an affected ACOS system's exposure. The CLI `web-service secure-server disable` and `web-service server disable` commands can be used to disable ACOS GUI services for HTTPS and HTTP; respectively.

*Note that disabling the GUI service will also disable the aXAPI RESTful API management service for the ACOS system, which will impact central management tools using the aXAPI service, including A10 aGalaxy and Harmony Controller.

Implement Identity Management Best Practices

Implementing best practice identity management solutions such as Single-Sign-On (SSO) with multi-factor authentication (MFA), Terminal Access Controller Access Control System (TACACS), or privilege access management (PAM) can reduce the likelihood of bad actors exploiting vulnerabilities that require authentication. For information about implementing SSO or TACACS with ACOS see the ACOS Hardening Guide available here: (Link).

Implement Network Deployment Best Practices

Implementing best practices when deploying network appliances can reduce the likelihood of an authenticated vulnerability being exploited by reducing overall attack surface. Best practices include ensuring management interfaces are confined to trusted internal networks, segmented management virtual local area networks (VLANs), or as part of a zero-trust deployment limiting access by user and application or protocol.

Hot Fix Mitigation - ACOS

Whenever possible, customers are advised to upgrade ACOS software to the latest available version. Customers who are unable to upgrade, may apply hotfixes that correspond to their release version.

Hot fixes for this vulnerability will not impact the normal functionality of an operational ACOS system, though other administrators connected to the system will be disconnected and need to reconnect after the hot fix is applied.

The following process details application of a hot fix to an ACOS system.

First download the hot fix image (i.e., hf-20230006.upg) from the A10 Networks Support software download site to a local device accessible to the ACOS system.

Next, determine the operational hard disk image (primary or secondary) of the system using the CLI command `show version` as shown below. Also confirm that the ACOS version is an affected ACOS release which supports a hot fix before proceeding. The operational image (primary or secondary) and the ACOS versions of the hard disk images can be located in the output of this command as shown below.

```
ACOS# show version
                        . . .
          Booted from Hard Disk primary image
                        . . .
          Hard Disk primary image (default) version 5.2.1-P7, build 160
          Hard Disk secondary image version 5.2.1-P3, build 70
                        . . .
ACOS(config)#
```

Next, apply the hot fix for the operational hard disk image of the system using the `upgrade` command in CLI config mode. Regardless of whether you specify the primary or the secondary image to be upgraded, the hot fix will only be applied for the hard disk image that is currently running.

NOTE: Note that a minimum of 2.8 GB of free space on the a10data partition is needed, and at least 50 KB of free space on the root partition is required.

NOTE: If prompted to save modified system configuration, answer “no” to avoid modifying system configuration while applying the hot fix.

NOTE: When prompted to reboot the system, answer “no” to avoid a restart of the ACOS system which could impact the running operations of the system.

```
ACOS(config)# admin-session clear all
2 out of 3 session(s) cleared.
ACOS(config)# upgrade hd pri use-mgmt-port scp://user@<ip-address>:/home/user/hf-20230006.upg
Password []?

System configuration has been modified. Save? [yes/no]:no
Do you want to reboot the system after the upgrade?[yes/no]:no
Upgrade ...
.................. Upgrade was successful (0 minutes 20 seconds) ACOS(config)#
```

To confirm that the hot fix was applied successfully, observe messages similar to the following in the ACOS log.

```
ACOS(config)# show log
Log Buffer: 30000
Sep 11 2023 04:47:18 Info        [SYSTEM]:Upgraded Hard Disk Primary image of ACOS from
root@10.67.2.211:/root/HF-20230006.upg.
Sep 11 2023 04:47:18 Info        [SYSTEM]:HF-20230006: Exiting
Sep 11 2023 04:47:18 Info        [SYSTEM]:HF-20230006: Security hot fix has been successfully applied
Sep 11 2023 04:46:59 Info        [SYSTEM]:HF-20230006: ACOS Hot fix is running
Sep 11 2023 04:46:58 Info        [SYSTEM]:upgrade: user=root;host=10.67.2.211;filepath=/root/HF-
20230006.upg;service=scp;primary=0
```

Similar to the above, the following are dialog and log messages for applying the hot fix to the secondary image of an ACOS system operating on the secondary image.

```
ACOS(config)# admin-session clear all
1 out of 2 session(s) cleared.
ACOS(config)# upgrade hd sec use-mgmt-port scp://user@<ip-address>:/home/user/hf-20230006.upg
Password []?

System configuration has been modified. Save? [yes/no]:no
Do you want to reboot the system after the upgrade?[yes/no]:no
Upgrade ...
....................... Upgrade was successful (0 minutes 21 seconds)

ACOS(config)# show log
Log Buffer: 30000
Sep 11 2023 05:24:58 Info        [SYSTEM]:Upgraded Hard Disk Secondary image of ACOS from
root@10.67.2.211:/root/HF-20230006.upg.
Sep 11 2023 05:24:58 Info        [SYSTEM]:HF-20230006: Exiting
Sep 11 2023 05:24:58 Info        [SYSTEM]:HF-20230006: Security hot fix has been successfully applied
Sep 11 2023 05:24:39 Info        [SYSTEM]:HF-20230006: ACOS Hot fix is running
Sep 11 2023 05:24:38 Info        [SYSTEM]:upgrade: user=root;host=10.67.2.211;filepath=/root/HF-
20230006.upg;service=scp;primary=0
```

Common reasons for hot fix application failures indicate the ACOS version is not exposed to the vulnerability and include the following.

- *Hot fix not compatible with the ACOS version installed on the hard disk image.*
- *Hot fix or updated ACOS version already installed on the hard disk image.*
- *Root partition of the hard disk is full (there will be an explanatory log message in this case).*
- *Hot fix was applied to a hard disk image that is not the booted image.*

Attempting to apply the hot fix for a disk image that is not the booted image will be display and log messages similar to the following.

```
ACOS(config)# upgrade hd sec use-mgmt-port scp://user@<ip-address>:/home/user/hf-20230006.upg
Password []?

System configuration has been modified. Save? [yes/no]:no
Do you want to reboot the system after the upgrade?[yes/no]:no
Failed to execute upgrade script

ACOS(config)# show log
Log Buffer: 30000
Nov 17 2020 07:23:00 Info        [SYSTEM]:HF-20230006: please run upgrade hd pri
Nov 17 2020 07:23:00 Info        [SYSTEM]:HF-20230006: Operation can only be applied to running
image: pri
```

Lastly, when it is convenient, reboot the system from the other hard disk image and repeat the process above.

Though the hot fix is persistent across system restarts, A10 Networks recommends that ACOS systems mitigated by applying hot fixes be updated to a resolved release, indicated above, at the earliest opportunity.

Software Updates

Software updates and hotfixes that address these vulnerabilities are available at the following URL:

https://support.a10networks.com/

Vulnerability Details

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

Vulnerability ID	Description
ZDI-CAN-17899	A10 Thunder ADC ShowTechDownloadView Directory Traversal Information Disclosure Vulnerability: • *A Path Traversal vulnerability exists in the ShowTechDownloadView class.* • *This vulnerability can be exploited by any authenticated user.* • *The vulnerability allows authenticated users to retrieve the content of arbitrary files.*

ZDI-CAN-17905	A10 Thunder ADC FileMgmtExport Directory Traversal Arbitrary File Read and Deletion Vulnerability:
	• *A Path Traversal vulnerability exists in the FileMgmtExport class.*
	• *This vulnerability can be exploited by any authenticated user.*
	• *The vulnerability allows authenticated users to:*
	  ○ *Retrieve the content of arbitrary files.*
	  ○ *Retrieve the whole directories (they will be returned as a TAR archive).*
	  ○ *Delete arbitrary and potentially critical A10 vThunder files leading to loss of service.*

Related Links

Ref #	General Link
[1]	https://www.zerodayinitiative.com/advisories/ZDI-CAN-17899
[2]	https://www.zerodayinitiative.com/advisories/ZDI-CAN-19705

Acknowledgements

A10 Networks would like to thank Trend Micro's Zero Day Initiative for reporting this vulnerability.

Modification History

Revision	Date	Description
1.0	2023-9-12	Initial Publication