ACOS/AGALAXY GUI RCE VULNERABILITY - CVE-2020-24384

PUBLISHED: NOVEMBER 9, 2020 | LAST UPDATE: NOVEMBER 20, 2020

SUMMARY

A vulnerability in the management Graphical User Interface (GUI) of A10 Networks' Advanced Core Operating System (ACOS) and aGalaxy systems could allow an unauthenticated, remote attacker with access to a management interface to execute arbitrary code on an affected system. Exploitation of this vulnerability could lead to partial or complete compromise of the ACOS or aGalaxy system.

This issue is exposed only on the management port or an otherwise configured management interface of an affected A10 system. The issue is not exposed on the system's data plane or management console.

A10 Networks strongly recommends that customers apply software updates or hot fixes indicated in this Security Advisory as soon as possible. Hot fixes for this vulnerability can be applied without impact to the normal functioning of an operational ACOS or aGalaxy system.

A10 Networks has assigned reference ID A10-2020-0006 to this vulnerability.

A10 Networks is not aware of malicious use of or attempts to exploit this vulnerability.

Item #	Vulnerability ID	Score Source	Score	Summary
1	CVE-2020-24384	CVSS 3.1	10.0 Critical	ACOS/aGalaxy GUI RCE Vulnerability

AFFECTED RELEASES

The table below indicates releases of ACOS and aGalaxy exposed to this vulnerability along with ACOS and aGalaxy releases and hot fixes that address it. ACOS and aGalaxy release families not indicated below are unaffected by this vulnerability.

Customers using affected ACOS or aGalaxy releases can overcome vulnerability exposures by updating to resolved releases or applying hot fixes identified in the table below. If the table does not list a corresponding resolved release (or hot fix), then no ACOS or aGalaxy release update (or hot fix) is currently available.

Product Family	Releases Affected			Releases Resolved or Unaffected	Hot Fix
ACOS	5.1.0	–	5.1.0-P3	5.1.0-P4, 5.2.0	HF-200006-3
ACOS	4.1.4	–	4.1.4-GR1-P4-SP1	4.1.4-GR1-P5	HF-200006-3
ACOS	4.1.2	–	4.1.2-P5-SP1	4.1.2-P5-SP2	HF-200006-3
ACOS	4.1.1	–	4.1.1-P13-SP1	4.1.1-P13-SP2	HF-200006-3
ACOS	4.1.100	–	4.1.100-P7	4.1.100-P8	HF-200006-3
ACOS	4.1.0	–	4.1.0-P13	4.1.0-P14	HF-200006-3
ACOS	4.0.3	–	4.0.3-P4		HF-200006-3
ACOS	4.0.0	–	4.0.1-P3		HF-200006-3
ACOS	3.2.5	–	3.2.5-P1	3.2.5-P2	HF-200006-3
ACOS	3.2.4	–	3.2.4-P5	3.2.4-P6	HF-200006-3
ACOS	3.2.3	–	3.2.3-P5	3.2.3-P6	HF-200006-3
ACOS	3.2.2	–	3.2.2-P8		HF-200006-3
aGalaxy-TPS	5.0.1	–	5.0.5	5.0.5-P1, 5.0.6	
aGalaxy-TPS	3.2.1	–	3.2.4	3.2.5	
aGalaxy-ADC	3.0.1	–	3.0.4-P3	3.0.4-P4	

WORKAROUNDS AND MITIGATIONS

RESTRICT GUI MANAGEMENT ACCESS

Common security best practices in the industry for network appliance management can enhance protection against remote malicious attacks. Limit the exploitable attack surface for critical infrastructure and networking equipment through the use of access lists or firewall filters to and from only trusted, administrative networks or hosts.

DISABLE REMOTE GUI MANAGEMENT - ACOS

Disabling the GUI management service, if it is not required, will mitigate an affected ACOS system's exposure to this vulnerability. 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 in this fashion will also disable the aXAPI RESTful API management service for the ACOS system, which can in turn impact central management tools using the aXAPI service, including A10 aGalaxy and Harmony Controller systems.

HOT FIX MITIGATION - ACOS

If it is not possible to update an ACOS system to a resolved release indicated above, the corresponding hot fix should be applied to mitigate this vulnerability for the system. *Hot fixes for this vulnerability will not impact the normal functioning 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.

To apply the hot fix to an ACOS system, first download the hot fix image (i.e., hf-200006-3.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 4.1.4-GR1-P4, build 47
          Hard Disk secondary image version 4.1.4-GR1-P2, build 72
                    . . .
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-200006-3.upg
Password []?

System configuration has been modified. Save? [yes/no]:no
Do you want to reboot the system after the upgrade?[yes/no]:no
Checking integrity of upgrade package ...
Upgrade file integrity checking passed
Done (0 minutes 1 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
Nov 17 2020 17:01:16 Info        [SYSTEM]:Upgraded Hard Disk Primary image of ACOS from user@<ip-
address>:/home/user/hf-200006-3.upg.
Nov 17 2020 17:01:16 Info        [SYSTEM]:HF-200006-3: Exiting
Nov 17 2020 17:01:16 Info        [SYSTEM]:HF-200006-3: Security hot fix has been successfully applied
Nov 17 2020 17:01:13 Info        [SYSTEM]:HF-200006-3: ACOS Hot fix for A10-2020-0006 - running
```

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-200006-3.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 25 seconds)

ACOS(config)# show log
Log Buffer: 30000
Nov 17 2020 11:06:00 Info        [SYSTEM]:Control CPU Usage OK. Current value is 35
Nov 17 2020 11:05:59 Info        [SYSTEM]:Upgraded Hard Disk Secondary image of ACOS from user@<ip-
address>:/home/user/hf-200006-3.upg.
Nov 17 2020 11:05:59 Info        [SYSTEM]:HF-200006-3: Exiting
Nov 17 2020 11:05:59 Info        [SYSTEM]:HF-200006-3: Security hot fix has been successfully applied
```

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-200006-3.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-200006-3: please run upgrade hd pri
Nov 17 2020 07:23:00 Info        [SYSTEM]:HF-200006-3: 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.

CONFIRMING THE HOT FIX

After successfully applying the hot fix, confirmation that the ACOS system is no longer exposed to this vulnerability can be determined by checking the hard disk images of the system using the `upgrade` command in CLI config mode. *Confirming application of the hot fix will not impact the normal functioning of an operational ACOS system*.

To check exposure of the image, first download the fix confirmation image (cf-200006-3.upg) from the A10 Networks Support software download site to a local device accessible to the ACOS system.

Next, check exposure for the hard disk image that is currently booted by using the `upgrade` command in CLI config mode.

NOTE: If prompted to save modified system configuration, answer "no" to avoid modifying system configuration while checking 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)# upgrade hd pri use-mgmt-port scp://user@<ip-address>:/home/user/cf-200006-3.upg
Password []?

System configuration has been modified. Save? [yes/no]:no
Do you want to reboot the system after the upgrade?[yes/no]:no
Checking integrity of upgrade package ...
Upgrade file integrity checking passed
Done (0 minutes 1 seconds)
ACOS(config)#
```

To confirm that the ACOS system is no longer exposed to the vulnerability, observe messages similar to the following in the ACOS log.

```
ACOS(config)# show log
Log Buffer: 30000
Nov 17 2020 07:20:38 Info        [SYSTEM]:Upgraded Hard Disk Primary image of ACOS from user@<ip-
address>:/home/user/cf-200006-3.upg.
Nov 17 2020 07:20:38 Info        [SYSTEM]:CF-200006-3: Exiting - no further action necessary
Nov 17 2020 07:20:38 Info        [SYSTEM]:CF-200006-3: Either the current running ACOS version is not
exposed to A10-2020-0006 or hot fix has already been applied
Nov 17 2020 07:20:38 Info        [SYSTEM]:CF-200006-3: Checking ACOS version for exposure to A10-2020-
0006
```

If desired, reboot the system from the other hard disk image and repeat the process above.

Attempting to run the confirmation for a disk image that is not the current booted image will be display and log messages similar to the following.

```
ACOS(config)# upgrade hd sec use-mgmt-port scp://user@<ip-address>:/mnt/bldimage/acos-hotfix/200006/cf-
200006-3.upg
Password []?

Do you want to reboot the system after the upgrade?[yes/no]:no
Failed to execute upgrade script
ACOS(config)# show log length 10
Log Buffer: 30000
Nov 17 2020 07:05:07 Info        [SYSTEM]:CF-200006-3: please run upgrade hd pri
Nov 17 2020 07:05:07 Info        [SYSTEM]:CF-200006-3: Operation can only be applied to running image:
pri
```

CONFIRMING EXPOSURE TO THE VULNERABILITY

The fix confirmation image described above can also be used to determine exposure of an ACOS system to this vulnerability prior to updating ACOS or applying the hot fix for the system. *Exposure confirmation for this vulnerability will not impact the normal functioning of an operational ACOS system.*

After performing the fix confirmation procedure using the `upgrade` command in CLI config mode, the ACOS log will include messages similar to the following for an exposed system.

```
ACOS(config)# show log
Log Buffer: 30000
Nov 18 2020 18:42:06 Info   [SYSTEM]:Upgraded Hard Disk Primary image of ACOS from user@<ip-
address>:/home/user/cf-200006-3.upg.
Nov 18 2020 18:42:06 Info   [SYSTEM]: CF-200006-3: Exiting
Nov 18 2020 18:42:06 Info   [SYSTEM]: CF-200006-3: please apply HF-200006-3 hot fix or update to
resolved ACOS release as soon as possible, please contact A10 support to get the resolved release
version
Nov 18 2020 18:42:06 Info   [SYSTEM]: CF-200006-3: The current running ACOS version IS EXPOSED to A10-
2020-0006
Nov 18 2020 18:42:06 Info   [SYSTEM]: CF-200006-3: Checking ACOS version for exposure to A10-2020-0006
```

The procedure should then be repeated to check the secondary image of the ACOS system.

SOFTWARE UPDATES

Software updates and hot fixes that address this vulnerability are available from A10 Networks Support via the following link. Hot fixes for this vulnerability are located near the bottom of the page, in the "*Other Updates and Tools*" section, and with the heading "*ACOS Security Hot Fixes – HF-200006-3*".

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

Customers with affected ACOS systems and who do not hold a support agreement with A10 Networks can obtain remediating hot fixes by contacting A10 Networks' Technical Assistance Center (TAC). Hot fixes will be provided free of charges or fees given the serial number of the ACOS system, reference to this CVE, and email address of the requesting party in possession of the ACOS system.

Customers with affected aGalaxy systems and who do not hold a support agreement with A10 Networks can obtain remediating updates by contacting A10 Networks' Technical Assistance Center (TAC). aGalaxy updates will be provided free of charges or fees given the serial number of the aGalaxy system, reference to this CVE, and email address of the requesting party in possession of the aGalaxy system.

Contact information for A10 Networks TAC can be found at https://www.a10networks.com/contact-us/tech-support.

VULNERABILITY DETAILS

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

Vulnerability ID	Description
CVE-2020-24384	The ACOS and aGalaxy management Graphical User Interfaces (GUIs) have a Remote Code Execution (RCE) vulnerability that could be used to compromise affected ACOS system. ACOS versions 3.2.x (including and after 3.2.2), 4.x, and 5.1.x are affected. aGalaxy versions 3.0.x, 3.2.x, and 5.0.x are affected.

RELATED LINKS

Ref #	General Link
[1]	A10 Networks Security Advisory - ACOS/aGalaxy GUI RCE Vulnerability - CVE-2020-24384
[2]	NIST NVD, CVE-2020-24384

ACKNOWLEDGEMENTS

A10 Networks would like to thank Todd Schertzing, Frederic Ladouceur, and Sam Wong of Xanthus Security, Inc. for reporting this vulnerability.

MODIFICATION HISTORY

Revision	Date	Description
1.3	2020-11-09	Initial Publication
1.4	2020-11-20	Revisions for version 3 of hot fix images.