CVE-2024-30368, CVE-2024-30369 – A10 ACOS COMMAND INJECTION REMOTE CODE EXECUTION & PRIVILEGE ESCALATION

PUBLISHED: MAY 28, 2024 | LAST UPDATE: MAY 28, 2024

Summary

A vulnerability in the management Graphical User Interface (GUI) of A10 Networks' Advanced Core Operating System (ACOS) systems could allow an authenticated attacker with access to a management interface to inject a command to be executed. This is CVE-2024-30368.

This issue is exposed only on the management port or an otherwise configured management interface of an affected A10 system and requires the attacker to be authenticated and logged into the system. The issue is not exposed on the system's data plane or management console or management Command Line Interface (CLI).

Using this exposure, it is possible to inject a command that will escalate the user privilege to root. This is CVE-2024-30369.

A10 Networks recommends that customers apply software updates indicated in this Security Advisory as soon as possible.

Trend Micro Zero Day Initiative research identified these issues as ZDI-CAN-22517 and ZDI-CAN-22754. A10 Networks assigned reference ID A10-2023-0020 and A10-2023-0021 to these vulnerabilities. These have since been assigned CVE-2024-30368 and CVE-2024-30369 respectively.

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

Item #	Vulnerability ID	Score Source	Score	Summary
1	CVE-2024-30368 ZDI-CAN-22517	CVSSv3	7.2 High	A10 Thunder ADC CsrRequestView Command Injection Remote Code Execution Vulnerability [1]
2	CVE-2024-30369 ZDI-CAN-22754	CVSSv3	7.8 High	A10 Thunder ADC Incorrect Permission Assignment Local Privilege Escalation Vulnerability [2]

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 can overcome vulnerability exposures by updating to the indicated resolved release. If the table does not list a corresponding resolved or unaffected release, then no ACOS release update is currently available.

Releases Affected			Releases Resolved or Unaffected
6.0.0	–	6.0.2-P1	6.0.3-P1
5.1.0	–	5.2.1-P9	5.2.1-P10
4.1.4	–	4.1.4-GR1-P13	4.1.4-GR1-P14

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.

Software Updates

Software updates that address these vulnerabilities are or will be published 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
CVE-2024-30368 ZDI-CAN-22517	A10 Thunder ADC CsrRequestView Command Injection Remote Code Execution Vulnerability. This advisory presents a Remote Code Execution issue in A10 vThunder. It can be exploited by a high-privileged user and it leads to a code execution as `a10user`. It can be chained with ZDI-CAN-22754 to escalated privileges to `root`.
CVE-2024-30369 ZDI-CAN-22754	A10 Thunder ADC Incorrect Permission Assignment Local Privilege Escalation Vulnerability. Local Privilege Escalation vulnerability exists in the A10 vThunder. It allows the user `a10user` to escalate privileges to `root`.

Related Links

Ref #	General Link
[1]	https://www.zerodayinitiative.com/advisories/ZDI-CAN-22517
[2]	https://www.zerodayinitiative.com/advisories/ZDI-CAN-22754

Acknowledgements

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

Modification History

Revision	Date	Description
1.0	2024-5-28	Initial Publication