TACACS+ LOGIN VULNERABILITY– A10-2025-0034

PUBLISHED: SEPTEMBER 30, 2025 | LAST UPDATE: SEPTEMBER 30, 2025

Summary

A10 Networks has discovered a security vulnerability in Advanced Core Operating System (ACOS) in conjunction with TACACS+ protocol that, if exploited, could result in unauthenticated user access. Exploitation requires impacted ACOS versions to be configured using TACACS, CLI management IPs to be configured without ACLs, and specialized knowledge of AXAPI authentication. If exploited, full access to the ACOS operating system may be gained via AXAPI. Authentication with RADIUS and LDAP are not affected. This vulnerability has been assigned to the internal case identifier of A10-2025-0034.

This vulnerability affects ACOS releases as indicated below and is being rated with a CVSS 3.1 score of 8.4 (High). A10 Networks is not aware of any existing malicious use of or attempts to exploit this vulnerability.

A10 Networks strongly recommends that you update exposed ACOS systems at the earliest opportunity.

Item #	Vulnerability ID	Score Source	Score	Summary
1	A10-2025-0034	CVSSv3.1	8.4 High	ACOS login issue when TACACS+ is configured as authentication protocol

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
6.0.4 – 6.0.7-P1 (b54 and below)	6.0.5-SP2, 6.0.7-P2

Workarounds and Mitigations

Restrict CLI 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.

Example Configuration

```
ip access-list management
        1 permit tcp 172.16.0.0 0.0.255.255 any eq 22
        1 permit tcp 172.16.0.0 0.0.255.255 any eq 443
        2 permit tcp 192.168.0.0 0.0.255.255 any eq 22
        2 permit tcp 192.168.0.0 0.0.255.255 any eq 443
!
```

```
interface management
       access-list name management in
       ip address 10.0.0.1 255.255.255.0
       ip default-gateway 10.0.0.250
```

Recommended Action

Along with hardening the management access on ACOS, we also recommend upgrading ACOS using the software update links below.

Disabling TACAS+ authentication protocol will mitigate exposure to this issue. Other authentication methods available include RADIUS, or local authentication.

Check for Exposure to Vulnerability with ACOS

After upgrading to the new recommended build, the new ACOS version can determine if the system was potentially exploited by this vulnerability.

In CLI mode, please follow the procedures below to determine if your system may have been compromised by this vulnerability.

1. To execute the checker, use the following CLI command or AXAPI Call.
    a. check (0/1) – Starts the checker
    b. days (1-90) – Number of days for the checker to go back.

CLI

```
ACOS(config)#accounting threat-logs check 30
```

AXAPI

```
POST: /axapi/v3/accounting/
```

```
{
    "accounting": {
        "threat-logs": {
            "check":1,
            "days":30
        }
    }
}
```

2. The checker will take some time to run after executing the command/call.
    a. The following command/call below can be used to determine the status of the checker
        i. Status – Shows the status of the checker
        ii. Result – 0 or 1, determines if the device may have been compromised.
        iii. Msg – Result message

CLI

```
ACOS(config)#show accounting threat-logs-report
status : in progress
result :
msg :
```

AXAPI

```
GET: /axapi/v3/accounting/threat-logs/oper
```

```
{
    "threat-logs": {
         "oper" : {
             "status":"in progress",
               "result: “”,
               "msg":"“
        }
    }
}
```

Once the checker has finished, run the above command again to see the outcome of the checker.
Device may have been compromised result

CLI

```
ACOS(config)#show accounting threat-logs-report
status : done
result : 1
msg : In the past 30 days, there were 9 potential instances that the device
may have been compromised by A10-2025-0034
```

AXAPI

```
GET: /axapi/v3/accounting/threat-logs/oper
```

```
{
   "threat-logs": {
       "oper" : {
           "status":”done",
             "result": 1,
             "msg":" In the past 30 days, there were 9 potential instances that
the device may have been compromised by A10-2025-0034 “
       }
    }
}
```

Device has not been compromised result

CLI

```
ACOS(config)show accounting threat-logs-report
status : done
result : 0
msg : In the past 30 days, there were 0 potential instances that the device
may have been compromised by A10-2025-0034
```

AXAPI

```
GET: /axapi/v3/accounting/threat-logs/oper
```

```
{
  "threat-logs": {
       "oper" : {
           "status":"done",
             "result": 0,
             "msg":" In the past 30 days, there were 0 potential instances that
the device may have been compromised by A10-2025-0034 “
        }
```

```
        }
    }
```

Software Updates

Software updates that address these vulnerabilities are or will be published at the following URL:

https://support.a10networks.com/

The ACOS 6.0.5-SP2 release is available here:

https://a10networks.sharefile.com/public/share/web-sf79ffba5325b408f88b1f9aac9377be3

Vulnerability Details

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

Vulnerability ID	Description
A10-2025-0034	A10 Networks has a login security vulnerability in ACOS when the TACACS+ protocol is used for authentication.

Related Links

Ref #	General Link
-	None

Acknowledgements

None

Modification History

Revision	Date	Description
1.0	2025-08-30	Initial Publication