MGMT ACLS CAN OVERRIDE MGMT SERVICE DISABLE COMMANDS

PUBLISHED: JULY 19, 2018 | LAST UPDATE: SEPTEMBER 24, 2018

SUMMARY

Services disabled on ACOS management interfaces can be inadvertently and unknowingly be enabled by Access Control List (ACL) rules defined for the services or interface. Three different types of ACL could potentially expose this vulnerability for in ACOS, including:

- Management Service ACLs (any interface),
- Management Service-Specific ACLs ("`mgmt`" interface only)
- Management Interface ACLs ("`mgmt`" interface only)

In such cases, the CLI commands would indicate the presence of management ACLs and "`off`" for the management service on management interfaces, even when the service was still available. This could allow a remote, man-in-the-middle attacker to eavesdrop on ACOS management sessions using unencrypted services, such as Telnet or HTTP, thought to be and indicated to be disabled in order to obtain credentials or other sensitive information and to modify traffic exchanged between a client and an ACOS device.

Item #	Vulnerability ID	Score Source	Score	Summary
1	A10-2017-0007 [(a)]	CVSS 3.0	7.6 High	Mgmt ACLs can Override Mgmt Service Disable Commands

[(a)] A10 Networks, Inc. assigned identifier.

AFFECTED RELEASES

The table below indicates releases of ACOS exposed to these vulnerabilities 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
4.1.4	–	4.1.4-P2	4.1.4-P3
4.1.2	–	4.1.2-P4	4.1.2-P5
4.1.1	–	4.1.1-P8	4.1.1-P9
4.1.0	–	4.1.0-P11	4.1.0-P12
3.1.0-P1	–	3.2.2-P5	3.2.2-P6, 3.2.3
2.8.2	–	2.8.2-P9	2.8.2-P10
2.7.2	–	2.7.2-P12	2.7.2-P13
2.7.1-GR1	–	2.7.1-GR1-Px	2.7.2-P13, 4.1.0-P12, 4.1.1-P9, 4.1.4-P3
2.6.1-GR1	–	2.6.1-GR1-P16	2.7.2-P13, 4.1.0-P12, 4.1.1-P9, 4.1.4-P3

WORKAROUNDS AND MITIGATIONS

MANAGEMENT SERVICE ACLS

ACOS management interfaces which are configured for ACLs can potentially expose disabled management services to this vulnerability. The configuration of such ACLs can be determined via the ACOS "`show management`" CLI command and the presence of numeric values in the ACL column.

The following is an example of a management service ACL configured for the "`eth1`" interface. For configurations with management service ACLs and with management services indicated as "`off`", verify that the disabled management services are indeed disabled on the interface, as described further below.

```
TH-Device#show management
       PING            SSH             Telnet          HTTP            HTTPS           SNMP            ACL
-------------------------------------------------------------------------------------------------------------
mgmt   on              on              off             off             on              on              -
eth1   on              on              off             off             on              on              10
eth2   on              off             off             off             off             off             -
...
```

MANAGEMENT SERVICE-SPECIFIC ACLS

Specific ACOS management services which are configured for ACLs can potentially expose disabled management services to this vulnerability. The configuration of such ACLs can be determined via the ACOS "`show management`" CLI command and presence the of an "`ACL`" indicator in service columns for the "`mgmt`" interface. Other ACOS interfaces are not exposed to this vulnerability.

The following is an example of a management service-specific ACL configured for the HTTPS service on the "`mgmt`" port. For configurations with management service-specific ACLs and with management services indicated as "`off`", verify that the disabled management services are indeed disabled on the "`mgmt`" interface, as described further below.

```
TH-Device#sh management
       PING            SSH             Telnet          HTTP            HTTPS           SNMP            ACL
-------------------------------------------------------------------------------------------------------------
mgmt   on              on              off             off             ACL 100         on              -
...
```

MANAGEMENT INTERFACE ACLS

Configuring ACLs for the ACOS management interface can also potentially expose disabled management services to this vulnerability. The configuration of such ACLs can be determined via the ACOS "`show run interface management`" CLI command and the presence of an "access-list" item for the corresponding "`management`" interface. Other ACOS interfaces are not exposed to this vulnerability. The configuration of services for the ACOS management interface can be determined via the ACOS "`show management`" CLI command.

The following is an example of a management interface ACL configured for ACOS management interface. For configurations with management interface ACLs and with management services indicated as "`off`", verify that the disabled management services are indeed disabled on the "`mgmt`" interface, as described further below.

```
TH-Device#show run interface management
!Section configuration: --- bytes
!
interface management
  ip address 192.168.213.89 255.255.255.0
  ip default-gateway 192.168.213.1
  access-list 100 in
!
TH-Device#sh management
       PING            SSH             Telnet          HTTP            HTTPS           SNMP            ACL
-------------------------------------------------------------------------------------------------------------
mgmt   on              on              off             off             on              on              -
...
```

VERIFYING MANAGEMENT SERVICES DISABLED

Verification that management services are disabled, as intended, can be performed with one or more of the following methods:

1. Inspection of the ACL rules, as identified in the discussions above, to ensure that they do not inadvertently permit traffic on TCP/UDP ports of disabled ACOS management services and ports.
2. Testing connectivity to TCP/UDP ports of disabled ACOS management services to ensure they are indeed disabled and unresponsive.

For environments where disabled management services are determined to still be accessible, review and update the management service, service-specific, and interface ACL rule definitions to ensure that ACOS management services intended to be disable are not otherwise permitted by the configured ACL rules.

SOFTWARE UPDATES

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

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
A10-2017-0007	Disabling an ACOS management service, for example … telnet via “enable-management service telnet/no management”, can inadvertently and unknowingly be actually left enabled by ACLs defined for the given management port. In such cases, the "sh management" command would indicate "off" for the management service on the port, even when the service was still available. Such can occur for any of the ACOS supported management services (e.g. ping, ssh, telnet, http, https, or snmp) and on any of the management ports (e.g. mgmt, eth1, eth2, etc).

RELATED LINKS

None

ACKNOWLEDGEMENTS

None

MODIFICATION HISTORY

Revision	Date	Description
1.0	2018-07-19	Initial Publication
2.0	2018-07-20	Corrected ACOS 2.7.2 affected and resolved releases.
3.0	2018-07-24	Updated summary discussion.
4.0	2018-07-24	Updated workarounds and mitigations. Updated 4.1.4 and 4.1.1 affected and resolved releases.
5.0	2018-09-24	Corrected to reflect 2.7.1-P13 as a resolved release for 2.6.1-GR1/2.7.1-GR1 families. Added 3.2.3 as a resolved release for the 3.2.x release family.