SK

Updated: August 25, 2021 **Document ID:** 1629910243056900

Bias-Free Langua

Cisco Security Advisory

Cisco NX-OS Software system login block-for Denial of Service Vulnerability

Medium

Advisory ID:
cisco-sa-nxos-login-blockfor-RwjGVEcu

First Published:
2021 August 25 16:00 GMT

Version 1.0: Final

Workarounds: No workarounds available

Cisco Bug IDs:
CSCuz49095 , CSCvw45963 , CSCvx74585

CVE-2021-1590

CVSS Score:
Base 5.3 **Click Icon to Copy Verbose Score**
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L/E:X/RL:X/RC:X

Download CSAF Download CVRF Email

Summary

A vulnerability in the implementation of the **system login block-for** command for Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause a login process to unexpectedly restart, causing a denial of service (DoS) condition.

This vulnerability is due to a logic error in the implementation of the **system login block-for** command when an attack is detected and acted upon. An attacker could exploit this vulnerability by performing a brute-force login attack

on an affected device. A successful exploit could allow the attacker to cause a login process to reload, which could result in a delay during authentication to the affected device.

Cisco has released software updates that address this vulnerability. There are no workarounds that address this vulnerability.

This advisory is available at the following link:
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-login-blockfor-RwjGVEcu

This advisory is part of the August 2021 Cisco FXOS and NX-OS Software Security Advisory Bundled Publication. For a complete list of the advisories and links to them, see Cisco Event Response: August 2021 Cisco FXOS and NX-OS Software Security Advisory Bundled Publication.

Affected Products

Vulnerable Products

At the time of publication, this vulnerability affected the following Cisco products if they were running a vulnerable release of Cisco NX-OS Software and had the **system login block-for** CLI command configured:

- MDS 9000 Series Multilayer Switches (CSCuz49095)
- Nexus 3000 Series Switches (CSCuz49095)
- Nexus 5500 Platform Switches (CSCvw45963)
- Nexus 5600 Platform Switches (CSCvw45963)
- Nexus 6000 Series Switches (CSCvw45963)
- Nexus 7000 Series Switches (CSCuz49095)
- Nexus 9000 Series Switches in standalone NX-OS mode (CSCuz49095)
- UCS 6200 Series Fabric Interconnects (CSCvx74585)
- UCS 6300 Series Fabric Interconnects (CSCvx74585)

The **system login block-for** command is disabled by default.

Note: The **login block-for** mode command was renamed **system login block-for** on certain Cisco NX-OS platforms and newer code trains. At the time of publication, this vulnerability applied to both forms of the command.

For information about which Cisco software releases are vulnerable, see the Fixed Software section of this advisory. See the bug ID(s) at the top of this advisory for the most complete and current information.

Determine the Device Configuration

NX-OS Software

To determine whether an affected device is configured with the **login block-for** or **system login block-for** CLI command, use the **show running-config | include block-for** command from the Cisco NX-OS CLI. If this command returns output, the device is considered vulnerable. The following example shows the output of the **show running-config | include block-for** command if the **system login block-for** command is configured on a device that is running Cisco NX-OS Software:

```
nexus# show running-config | include block-for
system login block-for 30 attempts 20 within 120
```

UCS Software

To determine whether a UCS 6200 Series or 6300 Series Fabric Interconnect is configured to block login requests, use the Cisco UCS Manager web UI to perform the following steps:

1. Go to the **Navigation** pane and click **Admin**.
2. Choose **Expand All > User Management > User Services > Login Profile**.
3. Go to the **Work** pane and see the setting of the **Enable** radio button in the **Admin State** field. If the **Enable** radio button is selected, the device is considered vulnerable.

The **Login Profile** configuration is disabled by default.

Products Confirmed Not Vulnerable

Only products listed in the Vulnerable Products section of this advisory are known to be affected by this vulnerability.

Cisco has confirmed that this vulnerability does not affect the following Cisco products:

- Firepower 1000 Series
- Firepower 2100 Series
- Firepower 4100 Series
- Firepower 9300 Security Appliances
- Nexus 1000 Virtual Edge for VMware vSphere
- Nexus 1000V Switch for Microsoft Hyper-V
- Nexus 1000V Switch for VMware vSphere
- Nexus 9000 Series Fabric Switches in Application Centric Infrastructure (ACI) mode
- UCS 6400 Series Fabric Interconnects

Details

The **system login block-for** feature can detect and protect against brute-force login attacks to the device. For information about the **system login block-for** command, see Configuring Login Parameters in the Configuring AAA chapter of Cisco Nexus 9000 Series NX-OS Security Configuration Guide, Release 9.3(x).

Indicators of Compromise

Exploitation of this vulnerability could cause the authentication, authorization, and accounting (AAA) daemon process to crash and generate an error message that is similar to the following:

```
%SYSMGR-2-SERVICE_CRASHED: Service "AAA Daemon" (PID 22769) hasn't caught
signal 11 (core will be saved).
```

This error message could have multiple causes. Customers who observe this message on a device are advised to contact their support organization to determine whether the message indicates that the device has been compromised by exploitation of this vulnerability.

Workarounds

There are no workarounds that address this vulnerability.

The device is only vulnerable if the **system login block-for** command is configured and a potential DoS attack was detected. If the command is removed using **no [system] login block-for** *seconds* **attempts** *tries* **within** *seconds*, the device is no longer vulnerable.

However, removing the **system login block-for** configuration weakens the security posture of the device. For additional information, see Configuring Login Parameters in the Configuring AAA chapter of Cisco Nexus 9000 Series NX-OS Security Configuration Guide, Release 9.3(x).

While this mitigation has been deployed and was proven successful in a test environment, customers should determine the applicability and effectiveness in their own environment and under their own use conditions. Customers should be aware that any workaround or mitigation that is implemented may negatively impact the functionality or performance of their network based on intrinsic customer deployment scenarios and limitations. Customers should not deploy any workarounds or mitigations before first evaluating the applicability to their own environment and any impact to such environment.

Fixed Software

When considering software upgrades, customers are advised to regularly consult the advisories for Cisco products, which are available from the Cisco Security Advisories page, to determine exposure and a complete upgrade solution.

In all cases, customers should ensure that the devices to be upgraded contain sufficient memory and confirm that current hardware and software configurations will continue to be supported properly by the new release. If the information is not clear, customers are advised to contact the Cisco Technical Assistance Center (TAC) or their contracted maintenance providers.

Cisco NX-OS Software

To help customers determine their exposure to vulnerabilities in Cisco NX-OS Software, Cisco provides the Cisco Software Checker to identify any Cisco Security Advisories that impact a specific Cisco NX-OS Software release and the earliest release that fixes the vulnerabilities that are described in each advisory ("First Fixed"). If applicable, the tool also returns the earliest release that fixes all the vulnerabilities described in all the advisories identified ("Combined First Fixed").

Customers can use the Cisco Software Checker to search advisories in the following ways:

- Choose the software, platform, and one or more releases
- Upload a .txt file that includes a list of specific releases
- Enter the output of the **show version** command

After initiating a search, customers can customize the search to include all Cisco Security Advisories or one or more specific advisories.

Customers can also use the following form to determine whether a release is affected by any Cisco Security Advisory by choosing the Cisco NX-OS Software and platform and then entering a release—for example, **7.0(3)I7(5)** for Cisco Nexus 3000 Series Switches or **14.0(1h)** for Cisco NX-OS Software in ACI mode:

Cisco NX-OS Software MDS 9000 Series Multilayer Switches

Enter Version Check

By default, the Cisco Software Checker includes results only for vulnerabilities that have a Critical or High Security Impact Rating (SIR). To include results for Medium SIR vulnerabilities, customers can use the Cisco Software Checker and check the **Medium** check box in the drop-down list under **Impact Rating** when customizing a search.

Cisco UCS Software

At the time of publication, the release information in the following table(s) was accurate. See the Details section in the bug ID(s) at the top of this advisory for the most complete and current information.

The left column lists Cisco software releases, and the right column indicates whether a release was affected by the vulnerability described in this advisory and which release included the fix for this vulnerability.

UCS 6200 and 6300 Series Fabric Interconnects: CSCvx74585

Cisco UCS Software Release	First Fixed Release for This Vulnerability
Earlier than 4.0	Migrate to a fixed release.
4.0	4.0(4m)
4.1	4.1(3d)
4.2	Not vulnerable.

Additional Resources

For help determining the best Cisco NX-OS Software release for a Cisco Nexus Switch, see the following Recommended Releases documents. If a security advisory recommends a later release, Cisco recommends following the advisory guidance.

- Cisco MDS Series Switches
- Cisco Nexus 1000V for VMware Switch
- Cisco Nexus 3000 Series Switches
- Cisco Nexus 5500 Platform Switches
- Cisco Nexus 5600 Platform Switches
- Cisco Nexus 6000 Series Switches
- Cisco Nexus 7000 Series Switches
- Cisco Nexus 9000 Series Switches
- Cisco Nexus 9000 Series ACI-Mode Switches

To determine the best release for Cisco UCS Software, see the Recommended Releases documents in the release notes for the device.

Exploitation and Public Announcements

The Cisco Product Security Incident Response Team (PSIRT) is not aware of any public announcements or malicious use of the vulnerability that is described in this advisory.

Source

This vulnerability was found during the resolution of a Cisco TAC support case.

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-login-blockfor-RwjGVEcu

Revision History

Version	Description	Section	Status	Date
1.0	Initial public release.	–	Final	2021-AUG-25

Legal Disclaimer

Cisco Security Vulnerability Policy

Subscribe to Cisco Security Notifications

Related to This Advisory