Release Notes for NX-OS Live Protect Shield

Release 10.6(3)

CVE-2026-20212 - Cisco Nexus 9000 Series Switches Silicon One Remote Code Execution Vulnerability

Live Protect Shield

Cisco has released Live Protect shield for CVE-2026-20212 to temporarily mitigate this vulnerability in Cisco NX-OS Software.

For information about Live Protect for Cisco NX-OS Software, see Cisco Nexus 9000 Series NX-OS Security Configuration Guide.

Note: Live Protect shield is a temporary mitigation to bridge the gap until software updates can be scheduled. To fully remediate this vulnerability, upgrade to a fixed software release, which can be found using the Cisco Software Checker.

Overview

A vulnerability in the Silicon One integration for Cisco Nexus 9000 Series Switches could allow an unauthenticated, remote attacker to execute code with root privileges.

For additional information, refer to the security advisory at the following link:

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-n9k-s1-rce-EH8dEtr

Attribute	Details
CVE ID	CVE-2026-20212
Shield ID	lp00031
Reference CDETS (IDs)	CSCwu32817
Shield File	`lp00031.lps-sone-secure-v1.lps`

Requirements

- **Affected switches**
    - N9324C-SE1U
    - N9348Y2C6D-SE1U
    - N9364E-SG2-O
    - N9364E-SG2-Q
    - N9396T12C-SE1
    - N9348Y12C-SE1
    - N9396Y12C-SE1
    - N9336C-SE1

  Note: The following switches are also affected but the Live Protect Shield is not supported on these platforms.
    - N9K-C9804
    - N9K-C9808

  Any Cisco Nexus Switches other than the above mentioned ones are not affected.
- **Access:** SSH, Telnet, or NXAPI access required for deployment.

Supported Releases

Cisco NX-OS Release 10.6(3)

© 2026 Cisco and/or its affiliates. All rights reserved.

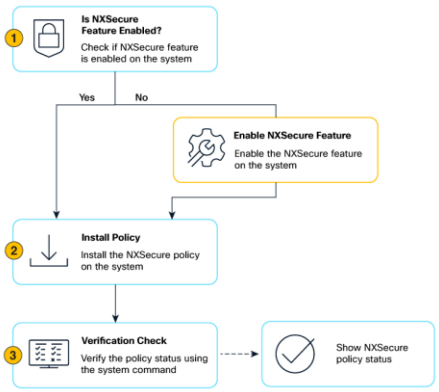
Shield behavior during Upgrade and Downgrade

Upgrade: When upgrading to NX-OS 10.6(4) or higher, shield operational mode transitions to N/A.

Downgrade: When downgrading to NX-OS 10.6(2), the shield will not be removed. You must remove the shied prior to downgrade using nxsecure policy remove method. For information about Live Protect for Cisco NX-OS Software, see Cisco Nexus 9000 Series NX-OS Security Configuration Guide.

Verification & Deployment Flow

The following process map outlines the validation path after policy deployment:



Verification Details

Policy Status

Use the following command to confirm the shield is in enforce mode:

```
switch# show nxsecure policy status

    Id                 Name                    Package                                                  Original
    Override  Current      Hits

    lp00031 lps-sone-secure          lp00031.lps-sone-secure-v1.lps enforce       none       enforce       1
```

Shield Log Output

To inspect the hit events, use:

```
switch# show nxsecure log lp00031

   Policy Id       : lp00031

   Policy Name     : lps-sone-secure

   Policy Severity : CRITICAL

   Policy Event    : Hit for CVE-2026-20212: Cisco Nexus 9000 Series Switches Silicon
   One Remote Code Execution Vulnerability

   Policy Event History(last 20 events):

   SNo             Time              Mode               Process

   1        2026 Aug 25 01:02:38   enforce          /usr/bin/nc
```

© 2026 Cisco and/or its affiliates. All rights reserved.

Shield Syslog

A syslog is received for every hit:

```
Syslog:

   2026 Aug 25 01:02:38 switch %APPMGR-2-NXSECURE_CRIT_THREAT: Shield ID: lp00031,
   Mode: enforce, Msg : Hit for CVE-2026-20212: Cisco Nexus 9000 Series Switches
   Silicon One Remote Code Execution Vulnerability^M
```

Reference

For detailed installation steps about Live Protect for Cisco NX-OS Software, see Cisco Nexus 9000 Series NX-OS Security Configuration Guide.

Documentation Feedback

To provide technical feedback on this document, or to report an error or omission, please send your comments to nexus9k-docfeedback@cisco.com. We appreciate your feedback.

Legal Information

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

© 2026 Cisco Systems, Inc. All rights reserved.