

Release Notes for NX-OS Live Protect Shield

CVE-2026-20032 - Cisco NX-OS Software Python Sandbox Escape Vulnerability

Live Protect Shield

Cisco has released Live Protect shield for [CVE-2026-20032](#) 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 Python interpreter of Cisco NX-OS Software could allow an authenticated, local attacker with low privileges to escape the Python sandbox and gain unauthorized access to the underlying operating system of an affected device.

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

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-mppe-dhKZAFgb>

Attribute	Details
CVE ID	CVE-2026-20032
Shield ID	lp00030
Reference bug (IDs)	CSCws98543
Shield File	lp00030-10.6.3-v1.lps

Requirements

- **Hardware:**
 - N9K-C92348GC-FX3
 - N9K-C9336C-FX2
 - N9K-C9332D-H2R
 - N9K-C9332D-GX2B
 - N9K-C9408
 - N9K-C93180YC-FX
 - N9K-C93108TC-FX
 - N9K-C9348GC-FXP
 - N9K-C93240YC-FX2
 - N9K-C93360YC-FX2
 - N9K-C93216TC-FX2
 - N9K-C93180YC-FX3S
 - N9K-C93180YC-FX3H

- N9K-C93180YC-FX3
- N9K-C93180YC-FX-24
- N9K-C93108TC-FX-24
- N9K-C93108TC-FX3
- N9K-C93108TC-FX3H
- N9K-C93108TC-FX3P
- N9K-C9348D-GX2A
- N9K-C9364D-GX2A
- N9K-C9364C-H1
- N9K-C9364C-GX
- N9K-C9364C-GX1
- N9K-C9348GC-FX3PH
- N9K-C9348GC-FX3
- N9K-C93400LD-H1
- N9K-C9336C-FX2-E
- N9K-9336C-SE1
- N9K-C9316D-GX
- N9K-C9336C
- N9K-C93600CD-GX
- N9396T12C-SE1
- N9324C-SE1U
- N9348Y2C6D-SE1U
- N9396Y12C-SE1
- N9348Y12C-SE1
- N9364E-SG2-O
- N9364E-SG2-Q
- N9336C-SE

- **Access:** SSH, Telnet, or NXAPI access required for shield deployment.

Supported Release(s)

Cisco NX-OS Release 10.6(3)

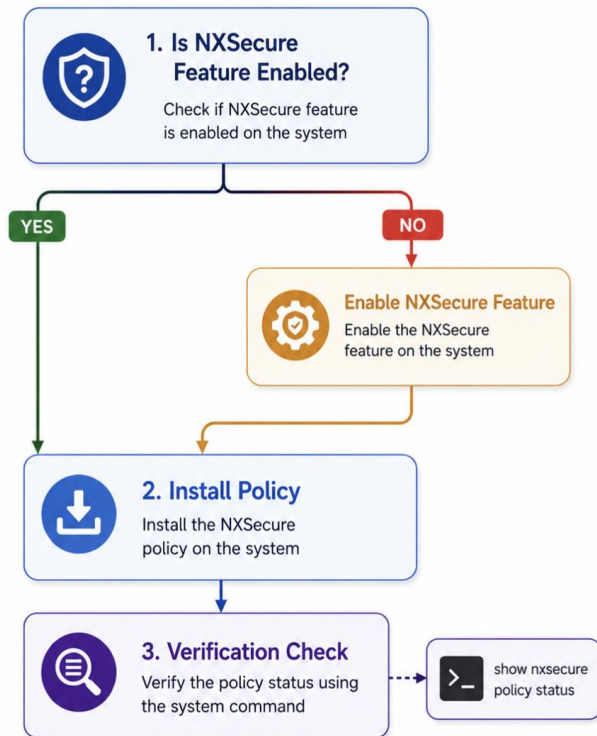
Shield behavior during Upgrade and Downgrade

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), shield will not be removed. User must remove the shield prior to downgrade using nxsecure policy remove method. Refer to [Live Protect 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
lp00030	cve-py-escape	lp00030-10.6.3-v1.lps	enforce	none	enforce	1

Shield Log Output

To inspect the hit events, use:

```
switch# show nxsecure log lp00030
```

```
Policy Id      : lp00030
Policy Name    : cve-py-escape
Policy Severity : CRITICAL
Policy Event   : Hit for CVE-2026-20032: Cisco NX-OS Software Python
                  Sandbox Escape Vulnerability
Policy Event History(last 20 events):
```

SNo	Time	Mode	Process
1	2026 Oct 01 16:36:23	enforce	/isan/bin/nxpython3

Shield Syslog

A syslog is received for every hit:

Syslog:

```
2026 Oct 1 22:06:23 switch %APPMGR-2-NXSECURE_CRIT_THREAT: Shield ID: 1p00030,  
Mode: enforce, Msg : Hit for CVE-2026-20032: Cisco NX-OS Software Python Sandbox  
Escape Vulnerability
```

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.