

The bridge to possible

Release Notes for NX-OS Live Protect Shield

CVE-2026-76501 - Cisco Nexus 9000 Series Switches SRv6 OAM (NGOAM) Remote Code Execution Vulnerability

Live Protect Shield

Cisco has released Live Protect shield for CVE-2026-76501 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 Segment Routing over IPv6 (SRv6) Operation, Administration, and Maintenance (OAM) feature of Cisco NX-OS Software, known as NGOAM, could allow an unauthenticated, remote attacker to execute arbitrary code with root privileges or cause a denial of service (DoS) on 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-ngoam-rce-LWKQ4BU

Attribute	Details
CVE ID	CVE-2026-76501
Shield ID	lp00036
Reference bug (IDs)	CSCwu19823
Shield File	`lp00036-10.6.3-v1.lps`

Requirements

- **Hardware**
  - N9K-9408
  - N9K-C9332D-H2R
  - N9K-C9364C-H1
  - N9K-C93400LD-H1
- **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

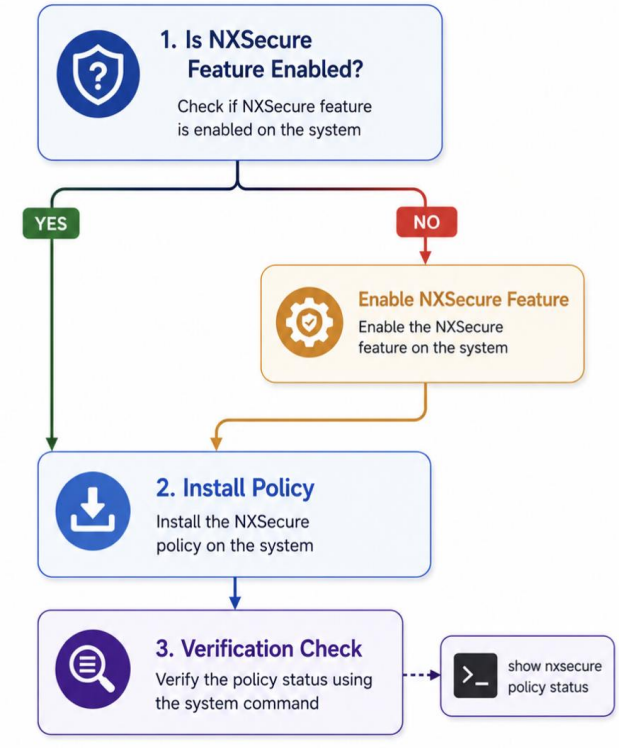
Upgrade: When upgrading to NX-OS 10.6(4) or higher, shield operational mode transitions to **N/A.**

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

Downgrade: When downgrading to NX-OS 10.6(2), shield will not be removed. User must remove the shied 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
    lp00036 cve-ngoam-srv-rce   lp00036-10.6.3-v1.lps   enforce     none     enforce       1
```

Shield Log Output

To inspect the hit events, use:

```
switch# show nxsecure log lp00036

   Policy Id       : lp00036
   Policy Name     : cve-ngoam-srv-rce
   Policy Severity : CRITICAL
   Policy Event    : Hit for CVE-2026-76501: Cisco Nexus 9000 Series
                     Switches SRv6 OAM (NGOAM) Remote Code Execution Vulnerability
   Policy Event History(last 20 events):
```

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

```
SNo            Time                Mode          Process
1        2026 Sep 29 06:52:33   enforce       /isan/bin/ngoam
```

Shield Syslog

A syslog is received for every hit:

Syslog:

```
2026 Sep 29 15:29:29 switch %APPMGR-2-NXSECURE_CRIT_THREAT: Shield ID: lp00036,
Mode: enforce, Msg : Hit for CVE-2026-76501: Cisco Nexus 9000 Series Switches SRv6
OAM (NGOAM) Remote Code Execution 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.