Cisco Integrated Management Controller Web-Based Management Interface Command Injection Vulnerability

**High**

**Advisory ID:**

cisco-sa-cimc-cmd-inj-bLuPcb

**First Published:**

2024 April 17 16:00 GMT

**Version 1.0:**

[Final](https://sec.cloudapps.cisco.com/security/center/resources/security_vulnerability_policy.html#final)

**Workarounds:**

No workarounds available

**Cisco Bug IDs:**

[CSCwi42996](https://bst.cloudapps.cisco.com/bugsearch/bug/CSCwi42996)

[CSCwi43001](https://bst.cloudapps.cisco.com/bugsearch/bug/CSCwi43001)

[CSCwi43005](https://bst.cloudapps.cisco.com/bugsearch/bug/CSCwi43005)

[More...](https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cimc-cmd-inj-bLuPcb)

**CVSS Score:**

[Base 8.7](https://sec.cloudapps.cisco.com/security/center/cvssCalculator.x?version=3.1&vector=CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:N)

CVE-2024-20356

CWE-78

[Download CSAF](https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cimc-cmd-inj-bLuPcb/csaf/cisco-sa-cimc-cmd-inj-bLuPcb.json)

[Email](mailto:?Subject=Cisco%20Security%20Advisory%20cisco-sa-cimc-cmd-inj-bLuPcb&Body=https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cimc-cmd-inj-bLuPcb)

**Summary**

* A vulnerability in the web-based management interface of Cisco Integrated Management Controller (IMC) could allow an authenticated, remote attacker with *Administrator*-level privileges to perform command injection attacks on an affected system and elevate their privileges to *root*.

This vulnerability is due to insufficient user input validation. An attacker could exploit this vulnerability by sending crafted commands to the web-based management interface of the affected software. A successful exploit could allow the attacker to elevate their privileges to *root*.

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-cimc-cmd-inj-bLuPcb>

**Affected Products**

* Vulnerable Products

This vulnerability affects the following Cisco products if they are running a vulnerable release of Cisco IMC in the default configuration:

* + 5000 Series Enterprise Network Compute Systems (ENCS)
  + Catalyst 8300 Series Edge uCPE
  + UCS C-Series M5, M6, and M7 Rack Servers in standalone mode
  + UCS E-Series Servers
  + UCS S-Series Storage Servers in standalone mode

Cisco appliances that are based on a preconfigured version of one of the Cisco UCS C-Series Servers that are in the preceding list are also affected by this vulnerability if they expose access to the Cisco IMC UI. At the time of publication, this included the following Cisco products:

* + Application Policy Infrastructure Controller (APIC) Servers
  + Business Edition 6000 and 7000 Appliances
  + Catalyst Center Appliances, formerly DNA Center
  + Cloud Services Platform (CSP) 5000 Series
  + Common Services Platform Collector (CSPC) Appliances
  + Connected Mobile Experiences (CMX) Appliances
  + Connected Safety and Security UCS Platform Series Servers
  + Cyber Vision Center Appliances
  + Expressway Series Appliances
  + HyperFlex Edge Nodes
  + HyperFlex Nodes in HyperFlex Datacenter without Fabric Interconnect (DC-NO-FI) deployment mode
  + IEC6400 Edge Compute Appliances
  + IOS XRv 9000 Appliances
  + Meeting Server 1000 Appliances
  + Nexus Dashboard Appliances
  + Prime Infrastructure Appliances
  + Prime Network Registrar Jumpstart Appliances
  + Secure Email Gateways1
  + Secure Email and Web Manager1
  + Secure Endpoint Private Cloud Appliances
  + Secure Firewall Management Center Appliances, formerly Firepower Management Center
  + Secure Malware Analytics Appliances
  + Secure Network Analytics Appliances
  + Secure Network Server Appliances
  + Secure Web Appliances1
  + Secure Workload Servers
  + Telemetry Broker Appliances

1. Cisco IMC is not directly accessible on these appliances, which significantly reduces the attack vector on these platforms.

For information about which Cisco software releases are vulnerable, see the [Fixed Software](https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cimc-cmd-inj-bLuPcb#fs) section of this advisory.

**Attention:** Simplifying the Cisco portfolio includes the renaming of security products under one brand: Cisco Secure. For more information, see [Meet Cisco Secure](https://www.cisco.com/c/en/us/products/security/secure-names.html).

Products Confirmed Not Vulnerable

Only products listed in the [Vulnerable Products](https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cimc-cmd-inj-bLuPcb#vp) section of this advisory are known to be affected by this vulnerability.

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

* + UCS B-Series Blade Servers
  + UCS C-Series Rack Servers managed by Cisco UCS Manager
  + UCS S-Series Storage Servers managed by Cisco UCS Manager
  + UCS X-Series Modular System

**Workarounds**

* There are no workarounds that address this vulnerability.

**Fixed Software**

* Cisco has released [free software updates](https://sec.cloudapps.cisco.com/security/center/resources/security_vulnerability_policy.html#ssu) that address the vulnerability described in this advisory. Customers with service contracts that entitle them to regular software updates should obtain security fixes through their usual update channels.

Customers may only install and expect support for software versions and feature sets for which they have purchased a license. By installing, downloading, accessing, or otherwise using such software upgrades, customers agree to follow the terms of the Cisco software license:  
<https://www.cisco.com/c/en/us/products/end-user-license-agreement.html>

Additionally, customers may only download software for which they have a valid license, procured from Cisco directly, or through a Cisco authorized reseller or partner. In most cases this will be a maintenance upgrade to software that was previously purchased. Free security software updates do not entitle customers to a new software license, additional software feature sets, or major revision upgrades.

The [Cisco Support and Downloads page](https://www.cisco.com/c/en/us/support/index.html) on Cisco.com provides information about licensing and downloads. This page can also display customer device support coverage for customers who use the My Devices tool.

When [considering software upgrades](https://sec.cloudapps.cisco.com/security/center/resources/security_vulnerability_policy.html#fixes), customers are advised to regularly consult the advisories for Cisco products, which are available from the [Cisco Security Advisories page](https://www.cisco.com/go/psirt), 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.

Customers Without Service Contracts

Customers who purchase directly from Cisco but do not hold a Cisco service contract and customers who make purchases through third-party vendors but are unsuccessful in obtaining fixed software through their point of sale should obtain upgrades by contacting the Cisco TAC: <https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html>

Customers should have the product serial number available and be prepared to provide the URL of this advisory as evidence of entitlement to a free upgrade.

Fixed Releases

In the following tables, the left column lists Cisco software releases. The right column indicates whether a release is affected by the vulnerability that is described in this advisory and the first release that includes the fix for this vulnerability. Customers are advised to upgrade to an appropriate [fixed software release](https://sec.cloudapps.cisco.com/security/center/resources/security_vulnerability_policy.html#fixes) as indicated in this section.

**5000 Series ENCS and Catalyst 8300 Series Edge uCPE**

**Note:** Upgrading Cisco IMC on Cisco 5000 Series ENCS and Cisco Catalyst 8300 Series Edge uCPE requires upgrading Cisco Enterprise NFV Infrastructure Software (NFVIS) on the platforms. Cisco IMC is upgraded as part of the firmware auto-upgrade process.

| **Cisco NFVIS Release** | **First Fixed Release** |
| --- | --- |
| 3.12 and earlier | Migrate to a fixed release. |
| 4.13 and earlier | 4.14.1 |

**UCS C-Series M5 Rack Server**

| **Cisco IMC Release** | **First Fixed Release** |
| --- | --- |
| 4.0 | Migrate to a fixed release. |
| 4.1 | 4.1(3n) |
| 4.2 | 4.2(3j) |
| 4.3 | 4.3(2.240009) |

**UCS C-Series M6 Rack Server**

| **Cisco IMC Release** | **First Fixed Release** |
| --- | --- |
| 4.2 | 4.2(3j) |
| 4.3 | 4.3(2.240009) 4.3(3.240022) |

**UCS C-Series M7 Rack Server**

| **Cisco IMC Release** | **First Fixed Release** |
| --- | --- |
| 4.3 | 4.3(3.240022) |

**UCS E-Series M2 and M3 Server**

| **Cisco IMC Release** | **First Fixed Release** |
| --- | --- |
| 3.1 and earlier | Migrate to a fixed release. |
| 3.2 | 3.2.15.3 |

**UCS E-Series M6 Server**

| **Cisco IMC Release** | **First Fixed Release** |
| --- | --- |
| 4.12 and earlier | 4.12.2 |

**UCS S-Series Storage Server**

| **Cisco IMC Release** | **First Fixed Release** |
| --- | --- |
| 4.0 | Migrate to a fixed release. |
| 4.1 | 4.1(3n) |
| 4.2 | 4.2(3k) |
| 4.3 | 4.3(2.240009) 4.3(3.240041) |

**Note:** For Cisco appliances that are based on a preconfigured version of one of the Cisco UCS C-Series Servers in the preceding tables, administrators can perform a direct upgrade of the Cisco IMC software to one of the fixed releases mentioned in the preceding tables. For instructions, see the [Cisco Host Upgrade Utility User Guide](https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/c/sw/lomug/4-2/b_cisco-host-upgrade-utility-user-guide-4-2/m_upgrading-the-firmware.html). The exceptions are the appliances that are listed in the following table. For these appliances, follow the instructions in the **Remediation** column:

| **Cisco Hardware Platform** | **First Fixed Cisco IMC Release** | **Remediation** |
| --- | --- | --- |
| IEC6400 Edge Compute Appliances | 4.2(3j) | Apply the HUU upgrade using **IEC6400-HUU-4.2.3j.img**. |
| Secure Email Gateways | 4.2(3j) | Install firmware update package (May 2024). |
| Secure Email and Web Manager | 4.2(3j) | Install firmware update package (May 2024). |
| Secure Endpoint Private Cloud Appliances | 4.3(2.240009) | Install firmware update **ucs-firmware-4.3.2.240009-1.rpm** (May 2024). |
| Secure Firewall Management Center Appliances | 4.3(2.240009) | Apply Hotfix [EZ](https://www.cisco.com/c/en/us/td/docs/security/firepower/hotfix/Firepower_Hotfix_Release_Notes/available-hotfixes.html#Cisco_Reference.dita_e5a104de-579f-48b7-adb6-0a72dc5183b7). |
| Secure Malware Analytics Appliances | 4.3(2.240009) | Upgrade to release 2.19.3 (July 2024). |
| Secure Network Analytics Appliances | 4.3(2.240009) | Install Update Patch **patch-common-SNA-FIRMWARE-20240305-v2-01.swu**. |
| Secure Network Server Appliances | 4.3(2.240009) | Apply the BIOS and HUU upgrade as documented in the Firmware Upgrade Guide for [SNS 3700 Series](https://www.cisco.com/c/en/us/td/docs/security/ise/sns3700hig/sns-37xx-firmware-4-x-xx_upgrade_guide.html#r_overview) or [SNS 3600 Series](https://www.cisco.com/c/en/us/td/docs/security/ise/sns3600hig/sns-36xx-firmware-4-x-xx_upgrade_guide.html#Cisco_Concept.dita_3e2c957e-62e6-4b2d-9f76-96ad121f29e1). |
| Secure Web Appliances | 4.2(3j) | Install firmware update package (May 2024). |
| Telemetry Broker Appliances | 4.3(2.240009) | Apply the update **patch-common-CTB-FIRMWARE-20240305.iso**. |

The Cisco Product Security Incident Response Team (PSIRT) validates only the affected and fixed release information that is documented in this advisory.

**Exploitation and Public Announcements**

* The Cisco PSIRT is not aware of any malicious use of the vulnerability that is described in this advisory.

**Source**

* Cisco would like to thank Aaron Thacker from LRQA Nettitude for reporting this vulnerability.

**URL**

* <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cimc-cmd-inj-bLuPcb>

**Revision History**

| **Version** | **Description** | **Section** | **Status** | **Date** |
| --- | --- | --- | --- | --- |
| 1.0 | Initial public release. | - | Final | 2024-APR-17 |

Cisco Integrated Management Controller Web-Based Management Interface Command Injection Vulnerability

**High**

**Advisory ID:**

cisco-sa-cimc-cmd-inj-bLuPcb

**First Published:**

2024 April 17 16:00 GMT

**Version 1.0:**

[Final](https://sec.cloudapps.cisco.com/security/center/resources/security_vulnerability_policy.html#final)

**Workarounds:**

No workarounds available

**Cisco Bug IDs:**

[CSCwi42996](https://bst.cloudapps.cisco.com/bugsearch/bug/CSCwi42996)

[CSCwi43001](https://bst.cloudapps.cisco.com/bugsearch/bug/CSCwi43001)

[CSCwi43005](https://bst.cloudapps.cisco.com/bugsearch/bug/CSCwi43005)

[More...](https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cimc-cmd-inj-bLuPcb)

**CVSS Score:**

[Base 8.7](https://sec.cloudapps.cisco.com/security/center/cvssCalculator.x?version=3.1&vector=CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:N)

CVE-2024-20356

CWE-78

[Download CSAF](https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cimc-cmd-inj-bLuPcb/csaf/cisco-sa-cimc-cmd-inj-bLuPcb.json)

[Email](mailto:?Subject=Cisco%20Security%20Advisory%20cisco-sa-cimc-cmd-inj-bLuPcb&Body=https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cimc-cmd-inj-bLuPcb)

**Summary**

* A vulnerability in the web-based management interface of Cisco Integrated Management Controller (IMC) could allow an authenticated, remote attacker with *Administrator*-level privileges to perform command injection attacks on an affected system and elevate their privileges to *root*.

This vulnerability is due to insufficient user input validation. An attacker could exploit this vulnerability by sending crafted commands to the web-based management interface of the affected software. A successful exploit could allow the attacker to elevate their privileges to *root*.

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-cimc-cmd-inj-bLuPcb>

**Affected Products**

* Vulnerable Products

This vulnerability affects the following Cisco products if they are running a vulnerable release of Cisco IMC in the default configuration:

* + 5000 Series Enterprise Network Compute Systems (ENCS)
  + Catalyst 8300 Series Edge uCPE
  + UCS C-Series M5, M6, and M7 Rack Servers in standalone mode
  + UCS E-Series Servers
  + UCS S-Series Storage Servers in standalone mode

Cisco appliances that are based on a preconfigured version of one of the Cisco UCS C-Series Servers that are in the preceding list are also affected by this vulnerability if they expose access to the Cisco IMC UI. At the time of publication, this included the following Cisco products:

* + Application Policy Infrastructure Controller (APIC) Servers
  + Business Edition 6000 and 7000 Appliances
  + Catalyst Center Appliances, formerly DNA Center
  + Cloud Services Platform (CSP) 5000 Series
  + Common Services Platform Collector (CSPC) Appliances
  + Connected Mobile Experiences (CMX) Appliances
  + Connected Safety and Security UCS Platform Series Servers
  + Cyber Vision Center Appliances
  + Expressway Series Appliances
  + HyperFlex Edge Nodes
  + HyperFlex Nodes in HyperFlex Datacenter without Fabric Interconnect (DC-NO-FI) deployment mode
  + IEC6400 Edge Compute Appliances
  + IOS XRv 9000 Appliances
  + Meeting Server 1000 Appliances
  + Nexus Dashboard Appliances
  + Prime Infrastructure Appliances
  + Prime Network Registrar Jumpstart Appliances
  + Secure Email Gateways1
  + Secure Email and Web Manager1
  + Secure Endpoint Private Cloud Appliances
  + Secure Firewall Management Center Appliances, formerly Firepower Management Center
  + Secure Malware Analytics Appliances
  + Secure Network Analytics Appliances
  + Secure Network Server Appliances
  + Secure Web Appliances1
  + Secure Workload Servers
  + Telemetry Broker Appliances

1. Cisco IMC is not directly accessible on these appliances, which significantly reduces the attack vector on these platforms.

For information about which Cisco software releases are vulnerable, see the [Fixed Software](https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cimc-cmd-inj-bLuPcb#fs) section of this advisory.

**Attention:** Simplifying the Cisco portfolio includes the renaming of security products under one brand: Cisco Secure. For more information, see [Meet Cisco Secure](https://www.cisco.com/c/en/us/products/security/secure-names.html).

Products Confirmed Not Vulnerable

Only products listed in the [Vulnerable Products](https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cimc-cmd-inj-bLuPcb#vp) section of this advisory are known to be affected by this vulnerability.

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

* + UCS B-Series Blade Servers
  + UCS C-Series Rack Servers managed by Cisco UCS Manager
  + UCS S-Series Storage Servers managed by Cisco UCS Manager
  + UCS X-Series Modular System

**Workarounds**

* There are no workarounds that address this vulnerability.

**Fixed Software**

* Cisco has released [free software updates](https://sec.cloudapps.cisco.com/security/center/resources/security_vulnerability_policy.html#ssu) that address the vulnerability described in this advisory. Customers with service contracts that entitle them to regular software updates should obtain security fixes through their usual update channels.

Customers may only install and expect support for software versions and feature sets for which they have purchased a license. By installing, downloading, accessing, or otherwise using such software upgrades, customers agree to follow the terms of the Cisco software license:  
<https://www.cisco.com/c/en/us/products/end-user-license-agreement.html>

Additionally, customers may only download software for which they have a valid license, procured from Cisco directly, or through a Cisco authorized reseller or partner. In most cases this will be a maintenance upgrade to software that was previously purchased. Free security software updates do not entitle customers to a new software license, additional software feature sets, or major revision upgrades.

The [Cisco Support and Downloads page](https://www.cisco.com/c/en/us/support/index.html) on Cisco.com provides information about licensing and downloads. This page can also display customer device support coverage for customers who use the My Devices tool.

When [considering software upgrades](https://sec.cloudapps.cisco.com/security/center/resources/security_vulnerability_policy.html#fixes), customers are advised to regularly consult the advisories for Cisco products, which are available from the [Cisco Security Advisories page](https://www.cisco.com/go/psirt), 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.

Customers Without Service Contracts

Customers who purchase directly from Cisco but do not hold a Cisco service contract and customers who make purchases through third-party vendors but are unsuccessful in obtaining fixed software through their point of sale should obtain upgrades by contacting the Cisco TAC: <https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html>

Customers should have the product serial number available and be prepared to provide the URL of this advisory as evidence of entitlement to a free upgrade.

Fixed Releases

In the following tables, the left column lists Cisco software releases. The right column indicates whether a release is affected by the vulnerability that is described in this advisory and the first release that includes the fix for this vulnerability. Customers are advised to upgrade to an appropriate [fixed software release](https://sec.cloudapps.cisco.com/security/center/resources/security_vulnerability_policy.html#fixes) as indicated in this section.

**5000 Series ENCS and Catalyst 8300 Series Edge uCPE**

**Note:** Upgrading Cisco IMC on Cisco 5000 Series ENCS and Cisco Catalyst 8300 Series Edge uCPE requires upgrading Cisco Enterprise NFV Infrastructure Software (NFVIS) on the platforms. Cisco IMC is upgraded as part of the firmware auto-upgrade process.

| **Cisco NFVIS Release** | **First Fixed Release** |
| --- | --- |
| 3.12 and earlier | Migrate to a fixed release. |
| 4.13 and earlier | 4.14.1 |

**UCS C-Series M5 Rack Server**

| **Cisco IMC Release** | **First Fixed Release** |
| --- | --- |
| 4.0 | Migrate to a fixed release. |
| 4.1 | 4.1(3n) |
| 4.2 | 4.2(3j) |
| 4.3 | 4.3(2.240009) |

**UCS C-Series M6 Rack Server**

| **Cisco IMC Release** | **First Fixed Release** |
| --- | --- |
| 4.2 | 4.2(3j) |
| 4.3 | 4.3(2.240009) 4.3(3.240022) |

**UCS C-Series M7 Rack Server**

| **Cisco IMC Release** | **First Fixed Release** |
| --- | --- |
| 4.3 | 4.3(3.240022) |

**UCS E-Series M2 and M3 Server**

| **Cisco IMC Release** | **First Fixed Release** |
| --- | --- |
| 3.1 and earlier | Migrate to a fixed release. |
| 3.2 | 3.2.15.3 |

**UCS E-Series M6 Server**

| **Cisco IMC Release** | **First Fixed Release** |
| --- | --- |
| 4.12 and earlier | 4.12.2 |

**UCS S-Series Storage Server**

| **Cisco IMC Release** | **First Fixed Release** |
| --- | --- |
| 4.0 | Migrate to a fixed release. |
| 4.1 | 4.1(3n) |
| 4.2 | 4.2(3k) |
| 4.3 | 4.3(2.240009) 4.3(3.240041) |

**Note:** For Cisco appliances that are based on a preconfigured version of one of the Cisco UCS C-Series Servers in the preceding tables, administrators can perform a direct upgrade of the Cisco IMC software to one of the fixed releases mentioned in the preceding tables. For instructions, see the [Cisco Host Upgrade Utility User Guide](https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/c/sw/lomug/4-2/b_cisco-host-upgrade-utility-user-guide-4-2/m_upgrading-the-firmware.html). The exceptions are the appliances that are listed in the following table. For these appliances, follow the instructions in the **Remediation** column:

| **Cisco Hardware Platform** | **First Fixed Cisco IMC Release** | **Remediation** |
| --- | --- | --- |
| IEC6400 Edge Compute Appliances | 4.2(3j) | Apply the HUU upgrade using **IEC6400-HUU-4.2.3j.img**. |
| Secure Email Gateways | 4.2(3j) | Install firmware update package (May 2024). |
| Secure Email and Web Manager | 4.2(3j) | Install firmware update package (May 2024). |
| Secure Endpoint Private Cloud Appliances | 4.3(2.240009) | Install firmware update **ucs-firmware-4.3.2.240009-1.rpm** (May 2024). |
| Secure Firewall Management Center Appliances | 4.3(2.240009) | Apply Hotfix [EZ](https://www.cisco.com/c/en/us/td/docs/security/firepower/hotfix/Firepower_Hotfix_Release_Notes/available-hotfixes.html#Cisco_Reference.dita_e5a104de-579f-48b7-adb6-0a72dc5183b7). |
| Secure Malware Analytics Appliances | 4.3(2.240009) | Upgrade to release 2.19.3 (July 2024). |
| Secure Network Analytics Appliances | 4.3(2.240009) | Install Update Patch **patch-common-SNA-FIRMWARE-20240305-v2-01.swu**. |
| Secure Network Server Appliances | 4.3(2.240009) | Apply the BIOS and HUU upgrade as documented in the Firmware Upgrade Guide for [SNS 3700 Series](https://www.cisco.com/c/en/us/td/docs/security/ise/sns3700hig/sns-37xx-firmware-4-x-xx_upgrade_guide.html#r_overview) or [SNS 3600 Series](https://www.cisco.com/c/en/us/td/docs/security/ise/sns3600hig/sns-36xx-firmware-4-x-xx_upgrade_guide.html#Cisco_Concept.dita_3e2c957e-62e6-4b2d-9f76-96ad121f29e1). |
| Secure Web Appliances | 4.2(3j) | Install firmware update package (May 2024). |
| Telemetry Broker Appliances | 4.3(2.240009) | Apply the update **patch-common-CTB-FIRMWARE-20240305.iso**. |

The Cisco Product Security Incident Response Team (PSIRT) validates only the affected and fixed release information that is documented in this advisory.

**Exploitation and Public Announcements**

* The Cisco PSIRT is not aware of any malicious use of the vulnerability that is described in this advisory.

**Source**

* Cisco would like to thank Aaron Thacker from LRQA Nettitude for reporting this vulnerability.

**URL**

* <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cimc-cmd-inj-bLuPcb>

**Revision History**

| **Version** | **Description** | **Section** | **Status** | **Date** |
| --- | --- | --- | --- | --- |
| 1.0 | Initial public release. | - | Final | 2024-APR-17 |