**Security Advisory 2021-043**

# Multiple Vulnerabilities in Cisco Products

***August 5, 2021 — v1.0***

**TLP:WHITE**

*History:*

- *05/08/2021 — v1.0 – Initial publication*

## Summary

On August 4, Cisco released multiple security updates to address several security vulnerabilities [1]. This list includes critical and high-severity vulnerabilities affecting Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers and high-severity vulnerabilities affecting:

- Cisco Small Business RV160 and RV260 Series VPN Routers.
- Cisco Network Services Orchestrator CLI Secure Shell Server.
- ConfD CLI Secure Shell Server.

The vulnerabilities in the web-based management interface of the Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an attacker to execute arbitrary code, cause a denial of service (DoS) condition and execute arbitrary commands [2]. Moreover, a vulnerability in Cisco Small Business RV160, RV160W, RV260, RV260P, and RV260W VPN Routers could allow an unauthenticated, remote attacker to execute arbitrary commands on the underlying operating system of an affected device [3].

The vulnerability affecting both Cisco Network Services Orchestrator CLI Secure Shell Server and ConfD CLI Secure Shell Server could allow an authenticated, local attacker to execute arbitrary commands [4, 5].

## Technical details

### CVE-2021-1609 - Remote Code Execution and Denial of Service Vulnerability

This critical vulnerability (CVSS score: 9.8 [2]) exists because HTTP requests are not properly validated. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to remotely execute arbitrary code on the device or cause the device to reload, resulting in a DoS condition [2].

### CVE-2021-1610 - Command Injection Vulnerability

This high-severity vulnerability (CVSS score: 7.2 [2]) in the web-based management interface of Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to execute arbitrary commands with root privileges on an affected device. This vulnerability exists because HTTP requests are not properly validated. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to execute arbitrary commands as *root* on the underlying operating system [2].

### CVE-2021-1602 - Remote Command Execution Vulnerability

This high-severity vulnerability (CVSS score: 8.2 [3]) in the web-based management interface of Cisco Small Business RV160, RV160W, RV260, RV260P, and RV260W VPN Routers could allow an unauthenticated, remote attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient user input validation. An attacker could exploit this vulnerability by sending a crafted request to the web-based management interface. A successful exploit could allow the attacker to execute arbitrary commands on an affected device using root-level privileges. Due to the nature of the vulnerability, only commands without parameters can be executed [3].

### CVE-2021-1572 - Privilege Escalation Vulnerability

This high severity vulnerability (CVSS score: 7.8 [4,5]) affects both Cisco Network Services Orchestrator (NSO) and ConfD CLI Secure Shell Server.

A vulnerability in Cisco Network Services Orchestrator (NSO) could allow an authenticated, local attacker to execute arbitrary commands at the level of the account under which Cisco NSO is running, which is *root* by default. To exploit this vulnerability, an attacker must have a valid account on an affected device. The vulnerability exists because the affected software incorrectly runs the SFTP user service at the privilege level of the account that was running when the NSO built-in Secure Shell (SSH) server for CLI was enabled. If the NSO built-in SSH server was not enabled, the device is not affected by this vulnerability. An attacker with low-level privileges could exploit this vulnerability by authenticating to an affected device and issuing a series of commands at the SFTP interface. A successful exploit could allow the attacker to elevate privileges to the level of the account under which Cisco NSO is running, which is *root* by default. Any user who can authenticate to the built-in SSH server may exploit this vulnerability. By default, all Cisco NSO users have this access if the server is enabled [4].

A vulnerability in ConfD could allow an authenticated, local attacker to execute arbitrary commands at the level of the account under which ConfD is running, which is commonly *root*. To exploit this vulnerability, an attacker must have a valid account on an affected device. The vulnerability exists because the affected software incorrectly runs the SFTP user service at the privilege level of the account that was running when the ConfD built-in Secure Shell (SSH)

server for CLI was enabled. If the ConfD built-in SSH server was not enabled, the device is not affected by this vulnerability. An attacker with low-level privileges could exploit this vulnerability by authenticating to an affected device and issuing a series of commands at the SFTP interface. A successful exploit could allow the attacker to elevate privileges to the level of the account under which ConfD is running, which is commonly *root*[5].

## Products affected

CVE-2021-1574 and CVE-2021-1576 vulnerabilities affect the following Cisco Small Business Routers if they are running a firmware release earlier than Release 1.0.03.22:

- RV340 Dual WAN Gigabit VPN Router
- RV340W Dual WAN Gigabit Wireless-AC VPN Router
- RV345 Dual WAN Gigabit VPN Router
- RV345P Dual WAN Gigabit POE VPN Router

CVE-2021-1602 vulnerability affects the following Cisco Small Business RV Series Routers if they are running firmware releases earlier than 1.0.01.04:

- RV160 VPN Routers
- RV160W Wireless-AC VPN Routers
- RV260 VPN Routers
- RV260P VPN Router with PoE
- RV260W Wireless-AC VPN Routers

CVE-2021-1572 vulnerability affects the following Cisco products and releases:

| Cisco Network Services Orchestrator CLI Secure Shell Server | ConfD CLI Secure Shell Server |
|---|---|
| Releases 5.4 through 5.4.3.1<br>Releases 5.5 through 5.5.2.2 | Releases 7.4 through 7.4.3<br>Releases 7.5 through 7.5.2 |

## Recommendations

Cisco has released software updates addressing these vulnerabilities [1, 2, 3, 4, 5].

There is no workaround addressing these vulnerabilities. However, mitigation steps are available for the vulnerability CVE-2021-1602 affecting Cisco NSO and ConfD CLI [4, 5].

CERT-EU recommends updating vulnerable applications as soon as possible.

## References


[1] https://tools.cisco.com/security/center/publicationListing.x

[2] https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv340-cmdinj-rcedos-pY8J3qfy

[3] https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-code-execution-9UVJr7k4

[4] https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nso-priv-esc-XXqRtTfT

[5] https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-confd-priv-esc-LsGtCRx4