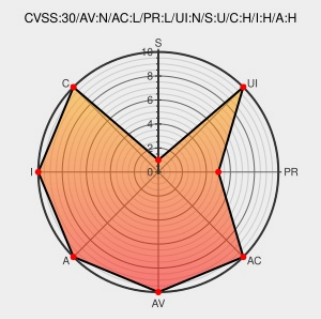
CVE-2018-0431

Published on: 10/05/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:49 PM UTC

CVE-2018-0431 - advisory for cisco-sa-20180905-cimc-injection

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Unified Computing System from Cisco contain the following vulnerability:

A vulnerability in the web-based management interface of Cisco Integrated Management Controller (IMC) Software could allow an authenticated, remote attacker to inject and execute arbitrary commands with root privileges on an affected device. The vulnerability is due to insufficient validation of command input by the affected software. 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 inject and execute arbitrary, system-level commands with root privileges on an affected device.

CVE-2018-0431 has been assigned by psirt@cisco.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **Cisco** - **Cisco Unified Computing System E-Series Software (UCSE)** version **n/a**

CVSS3 Score: 8.8 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	LOW	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: 9 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
Cisco Unified Computing System Command Injection Bug in CIMC Lets Remote Authenticated Users Execute Arbitrary Commands on the Target System - SecurityTracker	Third Party Advisory VDB Entry www.securitytracker.com text/html	SECTRACK 1041686
Cisco Integrated Management Controller Command Injection Vulnerability	Vendor Advisory tools.cisco.com text/html	CISCO 20180905 Cisco Integrated Management Controller Command Injection Vulnerability

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Cisco	Unified Computing System	2.0_base	All	All	All
Application	Cisco	Unified Computing System	3.0(3a)	All	All	All
Application	Cisco	Unified Computing System	3.0\(3a\)	All	All	All
Application	Cisco	Unified Computing System	3.1(3)	All	All	All
Application	Cisco	Unified Computing System	3.1\(3\)	All	All	All
Application	Cisco	Unified Computing System	2.0_base	All	All	All
Application	Cisco	Unified Computing System	3.0\(3a\)	All	All	All
Application	Cisco	Unified Computing System	3.1\(3\)	All	All	All

cpe:2.3:a:cisco:unified_computing_system:2.0_base:*:*:*:*:*:*:*:

cpe:2.3:a:cisco:unified_computing_system:3.0(3a):*:*:*:*:*:*:*:

cpe:2.3:a:cisco:unified_computing_system:3.0\(3a\):*:*:*:*:*:*:*:

cpe:2.3:a:cisco:unified_computing_system:3.1(3):*:*:*:*:*:*:*:

cpe:2.3:a:cisco:unified_computing_system:3.1\(3\):*:*:*:*:*:*:*:

cpe:2.3:a:cisco:unified_computing_system:2.0_base:*:*:*:*:*:*:*:

cpe:2.3:a:cisco:unified_computing_system:3.0\(3a\):*:*:*:*:*:*:*:

cpe:2.3:a:cisco:unified_computing_system:3.1\(3\):*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→