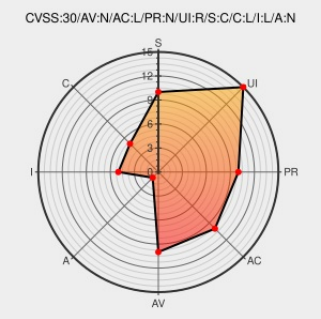
CVE-2019-15278

Published on: 01/25/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:44 PM UTC

CVE-2019-15278 - advisory for cisco-sa-20200108-finesse-xss

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



Certain versions of Finesse from Cisco contain the following vulnerability:

A vulnerability in the web-based management interface of Cisco Finesse could allow an unauthenticated, remote attacker to bypass authorization and access sensitive information related to the device. The vulnerability exists because the software fails to sanitize URLs before it handles requests. An attacker could exploit this vulnerability by submitting a crafted URL. A successful exploit could allow the attacker to gain unauthorized access to sensitive information.

CVE-2019-15278 has been assigned by psirt@cisco.com to track the vulnerability - currently rated as MEDIUM severity.

The Cisco Product Security Incident Response Team (PSIRT) is not aware of any public announcements or malicious use of the vulnerability that is described in this advisory.

Affected Vendor/Software: **Cisco** - **Cisco Finesse** version **n/a**

CVSS3 Score: 6.1 - MEDIUM

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

CVSS2 Score: 4.3 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	PARTIAL	NONE

CVE References

Description	Tags	Link
Cisco Finesse Cross-Site Scripting Vulnerability	Vendor Advisory tools.cisco.com text/html	CISCO 20200108 Cisco Finesse Cross-Site Scripting 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	Finesse	11.6(1)	-	All	All
Application	Cisco	Finesse	11.6\(1\)	-	All	All
Application	Cisco	Finesse	12.0(1)	-	All	All
Application	Cisco	Finesse	12.0\(1\)	-	All	All
Application	Cisco	Finesse	12.5(1)	All	All	All
Application	Cisco	Finesse	12.5\(1\)	All	All	All
Application	Cisco	Finesse	11.6\(1\)	-	All	All
Application	Cisco	Finesse	12.0\(1\)	-	All	All
Application	Cisco	Finesse	12.5\(1\)	All	All	All
Application	Cisco	Unified Contact Center Express	12.0(1)	All	All	All
Application	Cisco	Unified Contact Center Express	12.0\(1\)	All	All	All
Application	Cisco	Unified Contact Center Express	12.0\(1\)	All	All	All

cpe:2.3:a:cisco:finesse:11.6(1):-:*:*:*:*:*:*:

cpe:2.3:a:cisco:finesse:11.6\(1\):-:*:*:*:*:*:*:

cpe:2.3:a:cisco:finesse:12.0(1):-:*:*:*:*:*:*:

cpe:2.3:a:cisco:finesse:12.0\(1\):-:*:*:*:*:*:*:

cpe:2.3:a:cisco:finesse:12.5(1):*:*:*:*:*:*:*:

cpe:2.3:a:cisco:finesse:12.5\(1\):*:*:*:*:*:*:*:

cpe:2.3:a:cisco:finesse:11.6\(1\):-:*:*:*:*:*:*:

cpe:2.3:a:cisco:finesse:12.0\(1\):-:*:*:*:*:*:*:

cpe:2.3:a:cisco:finesse:12.5\(1\):*:*:*:*:*:*:*:

cpe:2.3:a:cisco:unified_contact_center_express:12.0(1):*:*:*:*:*:*:*:

cpe:2.3:a:cisco:unified_contact_center_express:12.0\(1\):*:*:*:*:*:*:*:

cpe:2.3:a:cisco:unified_contact_center_express:12.0\(1\):*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→