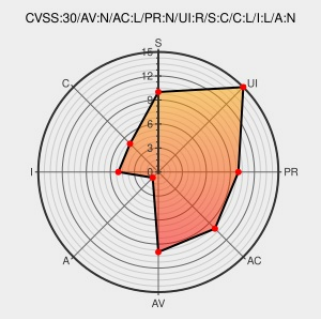
CVE-2017-6761

Published on: 08/07/2017 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:49 PM UTC

CVE-2017-6761

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 10.6(1) and 11.5(1) could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web-based management interface of an affected device. The vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of an affected device. An attacker could exploit this vulnerability by persuading a user of the interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the interface or allow the attacker to access sensitive browser-based information. Cisco Bug IDs: CSCvd96744.

CVE-2017-6761 has been assigned by psirt@cisco.com to track the vulnerability - currently rated as MEDIUM severity.

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 CVE-2017-6761 Cross Site Scripting Vulnerability	Third Party Advisory VDB Entry cve.report (archive) text/html	BID 100110
Cisco Bug: CSCvd96744 - Cisco Finesse Reflected Cross-Site Scripting Vulnerability	Vendor Advisory quickview.cloudapps.cisco.com text/html	CONFIRM quickview.cloudapps.cisco.com/quickview/bug/CSCvd96744
Cisco Finesse Input Validation Flaw Lets Remote Users Conduct Cross-Site Scripting Attacks - SecurityTracker	Third Party Advisory VDB Entry www.securitytracker.com text/html	SECTRACK 1039059
Cisco Finesse Reflected Cross-Site Scripting Vulnerability	Vendor Advisory tools.cisco.com text/html	CONFIRM tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170802-cf

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

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	10.6(1)	All	All	All
Application	Cisco	Finesse	10.6\(1\)	All	All	All
Application	Cisco	Finesse	11.5(1)	All	All	All
Application	Cisco	Finesse	11.5\(1\)	All	All	All
Application	Cisco	Finesse	10.6\(1\)	All	All	All
Application	Cisco	Finesse	11.5\(1\)	All	All	All

cpe:2.3:a:cisco:finesse:10.6(1):*:*:*:*:*:*:*:

cpe:2.3:a:cisco:finesse:10.6\(1\):*:*:*:*:*:*:*:

cpe:2.3:a:cisco:finesse:11.5(1):*:*:*:*:*:*:*:

cpe:2.3:a:cisco:finesse:11.5\(1\):*:*:*:*:*:*:*:

cpe:2.3:a:cisco:finesse:10.6\(1\):*:*:*:*:*:*:*:

cpe:2.3:a:cisco:finesse:11.5\(1\):*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

© CVE.report 2023 |
Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registred trademarks of The MITRE Corporation and the authoritative source of CVE content is MITRE's CVE web site. This site includes MITRE data granted under the following license.

CVE.report and Source URL Uptime Status status.cve.report