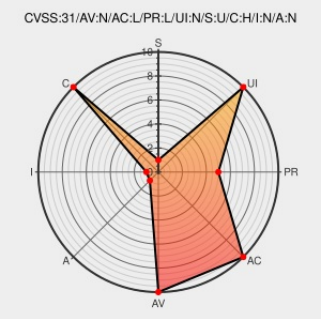
CVE-2018-15405

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

Last Modified on: 03/23/2021 11:24:27 PM UTC

CVE-2018-15405 - advisory for cisco-sa-20181003-imcs-ucsd-id

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



Certain versions of Ucs Director from Cisco contain the following vulnerability:

A vulnerability in the web interface for specific feature sets of Cisco Integrated Management Controller (IMC) Supervisor and Cisco UCS Director could allow an authenticated, remote attacker to access sensitive information. The vulnerability is due to an authorization check that does not properly include the access level of the web interface user. An attacker who has valid application credentials could exploit this vulnerability by sending a crafted HTTP request to the web interface. A successful exploit could allow the attacker to view sensitive information that belongs to other users. The attacker could then use this information to conduct additional reconnaissance attacks.

CVE-2018-15405 has been assigned by psirt@cisco.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **Cisco** - **Cisco Unified Computing System Director** version **n/a**

CVSS3 Score: 6.5 - MEDIUM

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

CVSS2 Score: 4 - MEDIUM

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

CVE References

Description	Tags	Link
Cisco Integrated Management Controller Supervisor and Cisco UCS Director Authenticated Web Interface Information Disclosure Vulnerability	Vendor Advisory tools.cisco.com text/html	CISCO 20181003 Cisco Integrated Management Controller Supervisor and Cisco UCS Director Authenticated Web Interface Information Disclosure Vulnerability
Cisco Unified Computing System Director Flaw Lets Remote Authenticated Users Obtain Potentially Sensitive Information - SecurityTracker	Third Party Advisory VDB Entry www.securitytracker.com text/html	SECTRACK 1041779

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Cisco	Ucs Director	2.1(0.0)	All	All	All
Application	Cisco	Ucs Director	2.1\(0.0\)	All	All	All
Application	Cisco	Ucs Director	6.6(1.0)	All	All	All
Application	Cisco	Ucs Director	6.6\(1.0\)	All	All	All
Application	Cisco	Ucs Director	2.1\(0.0\)	All	All	All
Application	Cisco	Ucs Director	6.6\(1.0\)	All	All	All

cpe:2.3:a:cisco:ucs_director:2.1(0.0):*:*:*:*:*:*:*:

cpe:2.3:a:cisco:ucs_director:2.1\(0.0\):*:*:*:*:*:*:*:

cpe:2.3:a:cisco:ucs_director:6.6(1.0):*:*:*:*:*:*:*:

cpe:2.3:a:cisco:ucs_director:6.6\(1.0\):*:*:*:*:*:*:*:

cpe:2.3:a:cisco:ucs_director:2.1\(0.0\):*:*:*:*:*:*:*:

cpe:2.3:a:cisco:ucs_director:6.6\(1.0\):*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

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