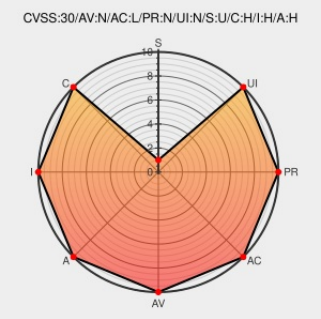
CVE-2019-1938

Published on: 08/21/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:48 PM UTC

CVE-2019-1938 - advisory for cisco-sa-20190821-ucsd-authbypass

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



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

A vulnerability in the web-based management interface of Cisco UCS Director and Cisco UCS Director Express for Big Data could allow an unauthenticated, remote attacker to bypass authentication and execute arbitrary actions with administrator privileges on an affected system. The vulnerability is due to improper authentication request handling. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow an unprivileged attacker to access and execute arbitrary actions through certain APIs.

CVE-2019-1938 has been assigned by psirt@cisco.com to track the vulnerability - currently rated as CRITICAL 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 Unified Computing System Director** version **6.7.3.0**

CVSS3 Score: 9.8 - CRITICAL

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

CVSS2 Score: 10 - HIGH

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

COMPLETE | COMPLETE | COMPLETE

CVE References

Description	Tags	Link
Cisco UCS Director and Cisco UCS Director Express for Big Data API Authentication Bypass Vulnerability	Vendor Advisory tools.cisco.com text/html	CISCO 20190821 Cisco UCS Director and Cisco UCS Director Express for Big Data API Authentication Bypass 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	Ucs Director	6.7.0.0	All	All	All
Application	Cisco	Ucs Director	6.7.1.0	All	All	All
Application	Cisco	Ucs Director	6.7.0.0	All	All	All
Application	Cisco	Ucs Director	6.7.1.0	All	All	All
Application	Cisco	Ucs Director Express For Big Data	3.7.0.0	All	All	All
Application	Cisco	Ucs Director Express For Big Data	3.7.1.0	All	All	All
Application	Cisco	Ucs Director Express For Big Data	3.7.0.0	All	All	All
Application	Cisco	Ucs Director Express For Big Data	3.7.1.0	All	All	All

cpe:2.3:a:cisco:ucs_director:6.7.0.0:*:*:*:*:*:*:*:

cpe:2.3:a:cisco:ucs_director:6.7.1.0:*:*:*:*:*:*:*:

cpe:2.3:a:cisco:ucs_director:6.7.0.0:*:*:*:*:*:*:*:

cpe:2.3:a:cisco:ucs_director:6.7.1.0:*:*:*:*:*:*:*:

cpe:2.3:a:cisco:ucs_director_express_for_big_data:3.7.0.0:*:*:*:*:*:*:*:

cpe:2.3:a:cisco:ucs_director_express_for_big_data:3.7.1.0:*:*:*:*:*:*:*:

cpe:2.3:a:cisco:ucs_director_express_for_big_data:3.7.0.0:*:*:*:*:*:*:*:

cpe:2.3:a:cisco:ucs_director_express_for_big_data:3.7.1.0:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

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