



CVE-2019-1866

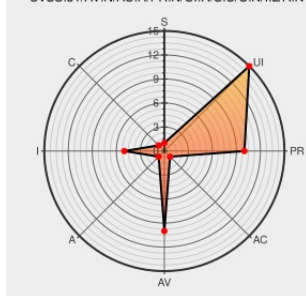
Published on: 04/13/2020 12:00:00 AM UTC

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

CVE-2019-1866 - advisory for CSCvm98833

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#)

CVSS:31/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:L/A:N



Certain versions of [Webex Business Suite 39](#) from [Cisco](#) contain the following vulnerability:

Cisco Webex Business Suite before 39.1.0 contains a vulnerability that could allow an unauthenticated, remote attacker to affect the integrity of the application. The vulnerability is due to improper validation of host header values. An attacker with a privileged network position, either a man-in-the-middle or by intercepting wireless network traffic, could

exploit this vulnerability to manipulate header values sent by a client to the affected application. The attacker could cause the application to use input from the header to redirect a user from the Cisco Webex Meetings Online site to an arbitrary site of the attacker's choosing.

CVE-2019-1866 has been assigned by [Cisco](#) psirt@cisco.com to track the vulnerability - currently rated as **LOW** 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 - Cisco Webex Business Suite** version < 39.1.0

CVSS3 Score: **3.7 - LOW**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	HIGH	NONE	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	NONE	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 Bug: CSCvm98833 - Cisco Webex Business Suite Host Header Injection Vulnerability	Vendor Advisory quickview.cloudapps.cisco.com text/html	 CISCO 20200413 Cisco Webex Business Suite Host Header Value Integrity Vulnerability

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	Webex Business Suite 39	All	All	All	All
Application	Cisco	Webex Business Suite 39	All	All	All	All

cpe:2.3:a:cisco:webex_business_suite_39:*:*:*:*:*:

cpe:2.3:a:cisco:webex_business_suite_39:*:*:*:*:*:

Discovery Credit

Cisco would like to thank Prasenjit Kanti Paul for reporting this vulnerability.

[← 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 registered 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](#)