Advisory Alert

Alert Number : AAA20201124 **Date :** November 24, 2020

Document Classification Level : Public Circulation Permitted

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Cisco	Medium	Multiple Vulnerabilities

Description

Affected Product	Cisco
Severity	Medium
Affected Vulnerability	Multiple Vulnerabilities
Description	Cisco has released security patch updates addressing multiple vulnerabilities that exists in their products. CVE-2020-3441 – Vulnerability discovered in Cisco Webex Meetings and Cisco Webex Meetings server caused by insufficient protection of sensitive participant information and it leads an un authenticated remote attacker to access sensitive information that transmits throughout the meeting. CVE-2020-3551 – Vulnerability was found in Cisco Identity service engine which could allow an unauthenticated attacker to cause a Cross site scripting attack against a user interface of an affected device. This is caused due to improper validation of user supplied input in web based management interface. CVE-2020-27122 – Vulnerability discovered in Microsoft Active Directory integration of Cisco Identity service engine leads an authenticated local attacker to elevate privileges on an affected device. The attacker will exploit this vulnerability by login in to the system using a crafted Active Directory account and successful exploitation could allow the attacker to obtain root privileges on the affected device.
Affected Products	Cisco Webex Meetings sites releases 40.11.3 and earlier Cisco Webex Meetings sites on Slow Channel releases 40.6.11 and earlier Cisco ISE releases 2.6 and 2.7
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webex-infodisc-4tvQzn4 https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-xss-euRCwX9 https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-priv-esc-fNZX8hHj

Disclaimer

The information provided herein is on "as is" basis, without warranty of any kind. FinCSIRT highly recommend to follow the company policies and procedures when applying the necessary patches with thorough testing and ensuring proper roll-back capabilities exists.