Advisory Alert

Alert Number: AAA20211007 **Date:** October 7, 2021

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Cisco	**High**	Multiple Vulnerabilities

Description

Affected Product	**Cisco**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2021-34698, CVE-2021-34748, CVE-2021-34775, CVE-2021-34776, CVE-2021-34777, CVE-2021-1594, CVE-2021-34710, CVE-2021-34735, CVE-2021-34788, CVE-2021-34766, CVE-2021-34744, CVE-2021-34757, CVE-2021-34706, CVE-2021-34702, CVE-2021-34711, CVE-2021-1534, CVE-2021-34782)
Description	Cisco has released Security Updates addressing multiple vulnerabilities that exist with various cisco products such as Denial of Service Vulnerability, Command Injection Vulnerability, Privilege Escalation Vulnerability, Shared Library Hijacking Vulnerability, XML External Entity Injection Vulnerability, Information Disclosure Vulnerability, Arbitrary File Read Vulnerability, and URL Filtering Bypass Vulnerability. It is highly recommended to apply necessary fixes provided on the official Cisco website at the earliest to avoid these security issues, and all Cisco users are encouraged to upgrade to the latest versions.
Affected Products	Cisco Web Security Appliance (WSA) Cisco Intersight Virtual Appliance Cisco Small Business 220 Series Smart Switches Cisco Identity Services Engine Cisco ATA 190 Series Cisco AnyConnect Secure Mobility Client Cisco SSM On-Prem Cisco Business 220 Series Smart Switches Cisco IP Phone Software Cisco Email Security Appliance Cisco DNA Center
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-wsa-dos-fmHdKswk https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ucsi2-command-inject-CGyC8y2R https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb220-lldp-multivuls-mVRUtQ8T https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-priv-esc-UwqPrBM3 https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ata19x-multivuln-A4J57F3 https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-anyconnect-lib-hija-cAFB7x4q https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ssm-priv-esc-5g35cdDJ https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-hardcoded-cred-MJCEXvX https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-xxe-inj-V4VSjEsX https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-info-disc-pNXtLhdp https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipphone-arbfileread-NPdtE2Ow https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-esa-url-bypass-sGcfsDrp https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-dnac-infodisc-KyC6YncS

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.