Advisory Alert

Alert Number: AAA20211105 **Date:** November 5, 2021

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Cisco	**Critical**	Multiple Vulnerabilities
Fortinet	**High**	Multiple Vulnerabilities

Description

Affected Product	Cisco
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2021-1500, CVE-2021-34701, CVE-2021-34731, CVE-2021-34739, CVE-2021-34741, CVE-2021-34773, CVE-2021-34774, CVE-2021-34784, CVE-2021-34795, CVE-2021-40112, CVE-2021-40113, CVE-2021-40115, CVE-2021-40119, CVE-2021-40120, CVE-2021-40124, CVE-2021-40126, CVE-2021-40127, CVE-2021-40128)
Description	Cisco has released security patch updates addressing multiple vulnerabilities that exists in multiple Cisco products. An attacker could use these vulnerabilities to gain access to systems and perform Denial of Service, Elevation of Privilege, Spoofing, Remote Code Execution, Data Manipulation, Security Restriction Bypass, Cross-Site Scripting and Information Disclosure. It is highly recommended by Cisco to apply necessary security fixes at earliest to avoid issues.
Affected Products	Cisco Policy Suite Cisco Catalyst PON Series Switches Cisco Business Series Switches Cisco Email Security Appliance Cisco Webex Cisco Umbrella Cisco Small Business Series Switches Cisco Small Business RV Series Routers Cisco Prime Cisco AnyConnect
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cps-static-key-JmS92hNv https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-catpon-multivulns-CE3DSYGr https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-smb-switches-tokens-UzwpR4e5 https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-esa-dos-JOm9ETfO https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webex-activation-3sdNFxcy https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-vmesh-openred-AGNRmf5 https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-videomesh-xss-qjm2BDQf https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-umbrella-user-enum-S7XfJwDE https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ucm-csrf-xrTkDu3H https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-smb-switches-web-dos-xMyFFkt8 https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sbrv-cmdinjection-Z5cWFdK https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-pi-epnm-xss-U2JK537j https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cucm-path-trav-dKCvktvO https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cspc-info-disc-KM3bGVL https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cpar-strd-xss-A4DCVETG https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-anyconnect-nam-priv-yCsRNUGT

Affected Product	Fortinet
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2020-15935, CVE-2020-12814, CVE-2021-42754, CVE-2021-36183, CVE-2020-15940, CVE-2021-36192, CVE-2021-26107, CVE-2021-41019, CVE-2021-32595, CVE-2021-36181, CVE-2021-36176, CVE-2021-36174, CVE-2021-36172, CVE-2021-32602, CVE-2021-41023, CVE-2021-41022, CVE-2021-36185, CVE-2021-36184, CVE-2021-36186, CVE-2021-36187, CVE-2020-15935)
Description	Fortinet has released security updates addressing multiple vulnerabilities that exists in their products including Execute unauthorized code or commands, Information disclosure, Denial of Service, privilege escalation, Improper Access Control and Cross-site scripting. Fortinet highly recommends to apply necessary security fixes at earliest to avoid issues.
Affected Products	FortiADC FortiSIEM FortiDDoS FortiDDoS-F FortiDDoS-CM FortiAnalyzer FortiClientMac FortiClientWindows FortiClientEMS FortiManager FortiOS FortiPortal FortiWLM FortiWebs
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.fortiguard.com/psirt/FG-IR-20-044 https://www.fortiguard.com/psirt/FG-IR-20-092 https://www.fortiguard.com/psirt/FG-IR-21-079 https://www.fortiguard.com/psirt/FG-IR-20-079 https://www.fortiguard.com/psirt/FG-IR-20-067 https://www.fortiguard.com/psirt/FG-IR-21-103 https://www.fortiguard.com/psirt/FG-IR-21-043 https://www.fortiguard.com/psirt/FG-IR-21-074 https://www.fortiguard.com/psirt/FG-IR-21-096 https://www.fortiguard.com/psirt/FG-IR-21-102 https://www.fortiguard.com/psirt/FG-IR-21-100 https://www.fortiguard.com/psirt/FG-IR-21-109 https://www.fortiguard.com/psirt/FG-IR-21-104 https://www.fortiguard.com/psirt/FG-IR-20-066 https://www.fortiguard.com/psirt/FG-IR-21-175 https://www.fortiguard.com/psirt/FG-IR-21-176 https://www.fortiguard.com/psirt/FG-IR-21-110 https://www.fortiguard.com/psirt/FG-IR-21-107 https://www.fortiguard.com/psirt/FG-IR-21-119 https://www.fortiguard.com/psirt/FG-IR-21-039 https://www.fortiguard.com/psirt/FG-IR-20-044

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.