Advisory Alert

Alert Number: AAA20210909 **Date:** September 9, 2021

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Cisco	**High**	Multiple Vulnerabilities
Citrix	**High**	Multiple Vulnerabilities

Description

Affected Product	Cisco
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2021-34713, CVE-2021-34720, CVE-2021-34718, CVE-2021-34719, CVE-2021-34728, CVE-2021-1440, CVE-2021-34708, CVE-2021-34709, CVE-2021-34771, CVE-2021-34737, CVE-2021-34721, CVE-2021-34722, CVE-2021-34785, CVE-2021-34786)
Description	Cisco has released updates addressing multiple vulnerabilities that exists in their products such as Arbitrary File Read and Write Vulnerability, Denial of Service Vulnerability, Information Disclosure Vulnerability, Privilege Escalation Vulnerability, Command Injection Vulnerabilities, Remote Code Execution Vulnerability. Cisco highly recommends to apply necessary security fixes to avoid issues.
Affected Products	Multiple Products
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://tools.cisco.com/security/center/publicationListing.x https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-npspin-QYpwdhFD https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipsla-ZA3SRrpP https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxr-scp-inject-QwZOCv2 https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxr-privescal-dZYMrKf https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-xrbgp-rpki-dos-gvmjqxbk https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-lnt-QN9mCzwn https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxr-infodisc-CjLdGMc5 https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxr-dhcp-dos-pjPVReLU https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxr-cmd-inj-wbZKvPxc https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-broadworks-dJ9JT67N

Affected Product	Citrix
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2021-28694, CVE-2021-28697, CVE-2021-28698, CVE-2021-28699, CVE-2021-28701)
Description	Citrix has released updates addressing multiple vulnerabilities that exists in Citrix Hypervisor such as Host denial of service, Host compromise. Citrix highly recommends to apply necessary security fixes to avoid issues.
Affected Products	Citrix Hypervisor
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.citrix.com/article/CTX325319

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.