Advisory Alert

Alert Number: AAA20210831 **Date:** August 31, 2021

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
VMware	Medium	Cross site scripting vulnerability
Cisco	Medium	Multiple Vulnerabilities

Description

Affected Product	VMware
Severity	Medium
Affected Vulnerability	Cross site scripting vulnerability (CVE-2021-22021)
Description	VMware has released security updates addressing Cross site scripting vulnerability that exists in their products. Using this flaw a malicious attacker with user privileges may be able to inject a malicious payload via the Log Insight UI which would be executed when the victim accesses the shared dashboard link.
Affected Products	VMware vRealize Log Insight VMware Cloud Foundation
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.vmware.com/security/advisories/VMSA-2021-0019.html

Affected Product	Cisco
Severity	Medium
Affected Vulnerability	Multiple vulnerabilities (CVE-2020-25681, CVE-2020-25682,CVE-2020-25683,CVE-2020-25684,CVE-2020-25685,CVE-2020-25686,CVE-2020-25687, CVE-2020-24586,CVE-2020-24587,CVE-2020-24588,CVE-2020-26139,CVE-2020-26140,CVE-2020-26141,CVE-2020-26142,CVE-2020-26143,CVE-2020-26144,CVE-2020-26145,CVE-2020-26146,CVE-2020-26147)
Description	Cisco has released security updates addressing multiple vulnerabilities that exists in their products. Successful exploitation of these vulnerabilities in vulnerable products could result in remote code execution, denial of service (DoS), forge DNS answers that can poison DNS caches and forge encrypted frames resulting in sensitive data exfiltration from a targeted device. Cisco highly recommends to apply necessary security fixes at earliest to avoid issues.
Affected Products	Multiple Cisco products
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-dnsmasq-dns-2021-c5mrdf3g https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-wifi-faf-22epcEWu

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.