TLP: WHITE

Advisory Alert

Alert Number : AAA20220224 **Date :** February 24, 2022

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

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

Description

Affected Product	**Redhat**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities
Description	Redhat has released security patch update addressing vulnerabilities that exist in their products **CVE-2021-44142 -** A remote attacker with write access to extended file attributes can execute arbitrary code with the privileges of smbd, typically root **CVE-2021-24407 -** Cyrus-sasl failure to properly escape SQL input allows an attacker to execute arbitrary SQL commands **CVE-2022-22816 -** A buffer over-read during initialization of ImagePath.Path **CVE-2022-22817 -** PIL.ImageMath.eval in Pillow before 9.0.0 allows evaluation of arbitrary expressions, such as ones that use the Python exec method.
Affected Products	Red Hat Virtualization 4 Red Hat Enterprise Linux 6 Red Hat Enterprise Linux 7 Red Hat Enterprise Linux 7.6 Red Hat Enterprise Linux 7.7 Red Hat Enterprise Linux 8
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/security/cve/CVE-2021-44142 https://access.redhat.com/security/cve/CVE-2022-24407 https://access.redhat.com/security/cve/CVE-2022-22816 https://access.redhat.com/security/cve/CVE-2022-22817

Affected Product	**Cisco**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities
Description	Cisco has released security patch update addressing vulnerabilities that exist in their products **CVE-2022-20623 -** A vulnerability in the rate limiter for Bidirectional Forwarding Detection (BFD) traffic of Cisco NX-OS Software for Cisco Nexus 9000 Series Switches could allow an unauthenticated, remote attacker to cause BFD traffic to be dropped on an affected device. **CVE-2022-20650 -** A vulnerability in the NX-API feature of Cisco NX-OS Software could allow an authenticated, remote attacker to execute arbitrary commands with root privileges. The vulnerability is due to insufficient input validation of user supplied data that is sent to the NX-API **CVE-2022-20624 -** A vulnerability in the Cisco Fabric Services over IP (CFSoIP) feature of Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of incoming CFSoIP packets **CVE-2021-1586 -** A vulnerability in the Multi-Pod or Multi-Site network configurations for Cisco Nexus 9000 Series Fabric Switches in Application Centric Infrastructure (ACI) mode could allow an unauthenticated, remote attacker to unexpectedly restart the device, resulting in a denial of service (DoS) condition. **CVE-2022-20625 -** A vulnerability in the Cisco Discovery Protocol service of Cisco FXOS Software and Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause the service to restart, resulting in a denial of service (DoS) condition.
Affected Products	Cisco Nexus 3000 Series Switches Cisco Nexus 5500 Platform Switches Cisco Nexus 5600 Platform Switches Cisco Nexus 6000 Series Switches Cisco Nexus 9000 Series Switches in standalone NX-OS Cisco Nexus 9200 and 9300 Platform Switches Cisco Nexus 9500 Series Switches Cisco FXOS Cisco NX-OS Software
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-bfd-dos-wGQXrzxn https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-nxapi-cmdinject-ULukNMZ2 https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cfsoip-dos-tpykyDr https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-n9kaci-tcp-dos-YXukt6gM https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cdp-dos-G8DPLWYG

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.