Advisory Alert

Alert Number: AAA20240126 **Date:** January 26, 2024

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Microsoft	**Critical**	Multiple Vulnerabilities
Cisco	**Critical**	Multiple Vulnerabilities
Juniper	**High**	Multiple Vulnerabilities
Drupal	**High**	Multiple Vulnerabilities
Cisco	**High, Medium**	Multiple Vulnerabilities
IBM	**High, Medium**	Multiple Vulnerabilities
OpenSSL	**Low**	Denial of Service Vulnerability

Description

Affected Product	**Microsoft**	
Severity	**Critical**	
Affected Vulnerability	Multiple Vulnerabilities(CVE-2024-0056, CVE-2024-0057, CVE-2024-20652, CVE-2024-20653, CVE-2024-20654, CVE-2024-20655, CVE-2024-20656, CVE-2024-20657, CVE-2024-20658, CVE-2024-20660, CVE-2024-20661, CVE-2024-20662, CVE-2024-20663, CVE-2024-20664, CVE-2024-20666, CVE-2024-20672, CVE-2024-20674, CVE-2024-20675, CVE-2024-20676, CVE-2024-20677, CVE-2024-20680, CVE-2024-20681, CVE-2024-20682, CVE-2024-20683, CVE-2024-20686, CVE-2024-20687, CVE-2024-20690, CVE-2024-20691, CVE-2024-20692, CVE-2024-20694, CVE-2024-20696, CVE-2024-20697, CVE-2024-20698, CVE-2024-20699, CVE-2024-20700, CVE-2024-21305, CVE-2024-21306, CVE-2024-21307, CVE-2024-21309, CVE-2024-21310, CVE-2024-21311, CVE-2024-21312, CVE-2024-21313, CVE-2024-21314, CVE-2024-21316, CVE-2024-21318, CVE-2024-21319, CVE-2024-21320, CVE-2024-21325, CVE-2024-21326, CVE-2024-21337, CVE-2024-21382, CVE-2024-21383, CVE-2024-21385, CVE-2024-21387)	
Description	Microsoft has released critical security updates for January 2024. This release includes fixes for several vulnerabilities across various Microsoft products. It is highly recommended that you apply these security patches immediately to protect your systems from potential threats.	
Affected Products	SQL Server .NET and Visual Studio Windows Scripting Windows Common Log File System Driver Windows ODBC Driver Windows Online Certificate Status Protocol (OCSP) SnapIn Visual Studio Windows Group Policy Microsoft Virtual Hard Drive Windows Message Queuing Microsoft Edge (Chromium-based) Azure Storage Mover Microsoft Office Windows Subsystem for Linux Windows Cryptographic Services	Windows Win32K Windows Win32 Kernel Subsystem Windows Hyper-V Unified Extensible Firmware Interface Microsoft Bluetooth Driver Remote Desktop Client Windows Cloud Files Mini Filter Driver .NET Framework Windows TCP/IP Windows Server Key Distribution Service Microsoft Office SharePoint Microsoft Identity Services Microsoft Devices Microsoft Edge for Android
Officially Acknowledged by the Vendor	Yes	
Patch/ Workaround Released	Yes	
Reference	https://msrc.microsoft.com/update-guide/releaseNote/2024-Jan	

Affected Product	**Cisco**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities(CVE-2024-20253, CVE-2024-20272)
Description	Cisco has released security updates addressing multiple vulnerabilities that exist in their product. **CVE-2024-20253** - An attacker could exploit this vulnerability by sending a crafted message to a listening port of an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the web services user. **CVE-2024-20272** - An attacker could exploit this vulnerability by uploading arbitrary files to an affected system. A successful exploit could allow the attacker to store malicious files on the system, execute arbitrary commands on the operating system, and elevate privileges to root. It is strongly recommends to apply the necessary remediation at your earliest to avoid issues.
Affected Products	Unified Communications Manager (Unified CM) (CSCwd64245) Unified Communications Manager IM & Presence Service (Unified CM IM&P) (CSCwd64276) Unified Communications Manager Session Management Edition (Unified CM SME) (CSCwd64245) Unified Contact Center Express (UCCX) (CSCwe18773) Unity Connection (CSCwd64292) Virtualized Voice Browser (VVB) (CSCwe18840) Cisco Unity Connection.
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cucm-rce-bWNzQcUm https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cuc-unauth-afu-FROYsCsD

Affected Product	**Juniper**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-21619, CVE-2023-36846, CVE-2024-21620, CVE-2023-36851, CVE-2024-21617)
Description	Juniper has released a security update for multiple vulnerabilities that exist in Juniper Junos OS. **CVE-2024-21619, CVE-2023-36846, CVE-2024-21620, CVE-2023-36851**- Multiple vulnerabilities in the J-Web component of Juniper Networks Junos OS on SRX Series and EX Series have been resolved through the application of specific fixes to address each vulnerability. These issues affect all versions of Juniper Networks Junos OS on SRX Series and EX Series. As each issue is fixed in different versions of Junos, please check the solution section and note that any earlier versions, and versions not mentioned to be fixed are affected. **CVE-2024-21617**- An Incomplete Cleanup vulnerability in Nonstop active routing (NSR) component of Juniper Networks Junos OS allows an adjacent, unauthenticated attacker to cause memory leak leading to Denial of Service (DoS). On all Junos OS platforms, when NSR is enabled, a BGP flap will cause memory leak. A manual reboot of the system will restore the services Juniper recommends to apply the necessary security updates at earliest to avoid issues.
Affected Products	All versions of Junos OS on SRX Series and EX Series. Junos OS 21.2, 21.3, 21.4, 22.1, 22.2, 22.3, 22.4.
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://supportportal.juniper.net/s/article/2024-01-Out-of-Cycle-Security-Bulletin-Junos-OS-SRX-Series-and-EX-Series-Multiple-vulnerabilities-in-J-Web-have-been-addressed?language=en_US https://supportportal.juniper.net/s/article/2024-01-Security-Bulletin-Junos-OS-BGP-flap-on-NSR-enabled-devices-causes-memory-leak-CVE-2024-21617?language=en_US

Affected Product	**Drupal**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities
Description	Drupal has released security patch updates addressing multiple vulnerabilities in Drupal Modules. Exploiting these vulnerabilities could lead to Access bypass, Information Disclosure. Drupal recommends to apply the necessary patch updates at your earliest to avoid issues.
.Affected Products	Swift Mailer Open Social distribution for Drupal 12.x Two-factor Authentication (TFA) for Drupal 8, 9, or 10
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.drupal.org/sa-contrib-2024-003 https://www.drupal.org/sa-contrib-2024-004 https://www.drupal.org/sa-contrib-2024-005 https://www.drupal.org/sa-contrib-2024-006

Affected Product	**Cisco**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities(CVE-2024-20263, CVE-2022-20716, CVE-2022-20930, CVE-2024-20270)
Description	Cisco has released security updates addressing multiple vulnerabilities that exist in their products. Successful exploitation of these vulnerabilities could lead to Cross-Site Scripting, ACL Bypass, and improper Access Control. It is recommends to apply the necessary remediation at your earliest to avoid issues.
.Affected Products	250 Series Smart Switches 350 Series Managed Switches 350X Series Stackable Managed Switches 550X Series Stackable Managed Switches Business 250 Series Smart Switches Business 350 Series Managed Switches SD-WAN vBond Orchestrator Software SD-WAN vEdge Cloud Routers SD-WAN vEdge Routers SD-WAN vManage Software SD-WAN vSmart Controller Software SD-WAN vBond Orchestrator Software BWCallCenter BWReceptionist
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cuc-xss-9TFuu5MS https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-bus-acl-bypass-5zn9hNJk https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sd-wan-file-access-VW36d28P https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-privesc-cli-xkGwmqKu https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-broadworks-xss-6syj82Ju

Affected Product	**IBM**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-46136,CVE-2023-43804, CVE-2023-35116, CVE-2023-34453, CVE-2023-2976, CVE-2022-3509, CVE-2022-3171, CVE-2022-25883 ,CVE-2023-45133 ,CVE-2023-43642, CVE-2023-37920, CVE-2023-34455, CVE-2023-34454, CVE-2023-33201)
Description	IBM has released security updates addressing Multiple Vulnerabilities that exist in QRadar SIEM. Successful exploitation of above vulnerabilities could lead to directory traversal, improper access controls, arbitrary code execution, and denial of service. IBM recommends to apply the necessary patch updates at your earliest to avoid issues.
.Affected Products	IBM Security QRadar SIEM
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/bulletin/search/?q=QRadar%20SIEM

Affected Product	**OpenSSL**
Severity	**Low**
Affected Vulnerability	Denial of Service Vulnerability (CVE-2024-0727)
Description	OpenSSL has released a security updates to address Denial of Service that exist in the Applications loading files in the PKCS12 format from untrusted sources might terminate abruptly. A file in PKCS12 format can contain certificates and keys and may come from an untrusted source. The PKCS12 specification allows certain fields to be NULL, but OpenSSL does not correctly check for this case. This can lead to a NULL pointer dereference that results in OpenSSL crashing. If an application processes PKCS12 files from an untrusted source using the OpenSSL APIs then that application will be vulnerable to this issue. OpenSSL recommends to apply necessary security fixes at earliest to avoid issues
.Affected Products	OpenSSL 3.2, 3.1, 3.0, 1.1.1 and 1.0.2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.openssl.org/news/secadv/20240125.txt

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.