Advisory Alert

Alert Number: AAA20220616 **Date:** June 16, 2022

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Cisco	**Critical**	Multiple Vulnerabilities
Cisco	**High, Medium**	Multiple Vulnerabilities
IBM	**High**	Multiple Vulnerabilities
Microsoft	**High**	Multiple Vulnerabilities

Description

Affected Product	**Cisco**
Severity	**Critical**
Affected Vulnerability	Multiple vulnerabilities (CVE-2022-20798, CVE-2022-20825)
Description	Cisco has released security updates addressing multiple vulnerabilities in their products. **CVE-2022-20798** - The Vulnerability is caused due to improper authentication checks when an affected device uses Lightweight Directory Access Protocol (LDAP) for external authentication. The vulnerability can be exploited by entering a specific input on the login page of the affected device. A successful exploit could allow the attacker to gain unauthorized access to the web-based management interface of the affected device. **CVE-2022-20825** - An unauthenticated remote attacker can execute arbitrary code or unexpectedly restart Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers due to a vulnerability in web-based management interface of the routers. Unexpected restarts cause denial of service. This vulnerability is due to insufficient user input validation of incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted request to the web-based management interface. A successful exploit could allow the attacker to execute arbitrary commands on an affected device using root-level privileges. Customers are encouraged to migrate to the Cisco Small Business RV132W, RV160, or RV160W Routers. Cisco recommends to apply necessary security fixes at earliest to avoid issues.
Affected Products	Cisco Secure Email Web Manager Cisco Email Security Appliance (ESA) RV110W Wireless-N VPN Firewall RV130 VPN Router RV130W Wireless-N Multifunction VPN Router RV215W Wireless-N VPN Router
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sma-esa-auth-bypass-66kEcxQD https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv-overflow-s2r82P9v

Affected Product	**Cisco**
Severity	**High, Medium**
Affected Vulnerability	Multiple vulnerabilities (CVE-2022-20664, CVE-2022-20819, CVE-2022-20817, CVE-2022-20733)
Description	Cisco has released security updates addressing multiple vulnerabilities in their products. This would lead attackers to cause information disclosure, authentication bypass and duplicate key vulnerability. Cisco recommends to apply necessary security fixes at earliest to avoid issues.
Affected Products	Cisco Secure Email, Web Manager, Cisco Email Security Appliance (ESA), Cisco ISE 2.2 and earlier, 2.3, 2.4, 2.6, 3.1 ATA 187 Analog Telephone Adapter Unified IP Phone 6911 Unified IP Phone 6921 Unified IP Phone 6941 Unified IP Phone 6945 Unified IP Phone 6961 Unified IP Phone 8941 Unified IP Phone 8945 Unified IP Phone 8961 Unified IP Phone 9951 Unified IP Phone 9971
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-esasma-info-dsc-Q9tLuOvM https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-info-disclosure-Os6fSd6N https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cp6901-dup-cert-82jdJGe4 https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ISE-SAML-nuukMPf9

Affected Product	**IBM**
Severity	**High**
Affected Vulnerability	Multiple vulnerabilities (CVE-2019-20916, CVE-2021-3572, CVE-2018-20225)
Description	IBM has released a security update for multiple vulnerabilities that have been discovered in Pip, which is used by IBM QRadar Advisor With Watson to manage python packages. **CVE-2019-20916 –** When a URL is given in an install command, the pip package for Python before 19.2 allows Directory Traversal, because a Content-Disposition header can have ../ in a filename, as demonstrated by overwriting the /root/.ssh/authorized_keys file. This occurs in _download_http_url in _internal/download.py. **CVE-2021-3572** - A remote authenticated attacker could bypass security restrictions using the pip package for Python, due to improper handling of Unicode separators in git references. An attacker could exploit this by creating a specially crafted tag to install a different revision on a repository. **CVE-2018-20225** - A local attacker could use Pip to run arbitrary code on the system, due to a flaw in the --extra-index-url option. An attacker could exploit this vulnerability by sending a specially crafted request to execute arbitrary code on the system. IBM highly recommends to apply necessary security fixes at earliest to avoid issues
Affected Products	QRadar Advisor With Watson 2.5 – QRadar Advisor With Watson 2.6.2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/6595273

Affected Product	**Microsoft**	
Severity	**High**	
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-2007, CVE-2022-2008, CVE-2022-2010, CVE-2022-2011, CVE-2022-21123, CVE-2022-21125, CVE-2022-21127, CVE-2022-21166, CVE-2022-22018, CVE-2022-22021, CVE-2022-29111, CVE-2022-29119, CVE-2022-29143, CVE-2022-29149, CVE-2022-30136 CVE-2022-30137, CVE-2022-30139, CVE-2022-30140, CVE-2022-30141 CVE-2022-30142, CVE-2022-30143, CVE-2022-30145, CVE-2022-30146 CVE-2022-30148, CVE-2022-30149, CVE-2022-30150, CVE-2022-30151 CVE-2022-30153, CVE-2022-30154, CVE-2022-30155, CVE-2022-30157 CVE-2022-30158, CVE-2022-30159, CVE-2022-30161, CVE-2022-30162, CVE-2022-30163, CVE-2022-30164, CVE-2022-30165, CVE-2022-30167, CVE-2022-30168, CVE-2022-30171, CVE-2022-30172, CVE-2022-30173, CVE-2022-30174, CVE-2022-30177, CVE-2022-30178, CVE-2022-30179, CVE-2022-30180, CVE-2022-30184, CVE-2022-30188, CVE-2022-30189, CVE-2022-30193, CVE-2022-32230)	
Description	Microsoft has issued Security Updates addressing multiple vulnerabilities that exists in variety of Microsoft products, features, and roles. Updates include defense-in-depth updates to help strengthen security-related aspects, in addition to security improvements for the vulnerabilities. Microsoft strongly advises to apply security fixes at earliest to avoid problems.	
Affected Products	NET and Visual Studio Azure OMI Azure Real Time Operating System Azure Service Fabric Container Intel Microsoft Edge (Chromium-based) Microsoft Office Microsoft Office Excel Microsoft Office SharePoint Microsoft Windows ALPC Microsoft Windows Codecs Library Remote Volume Shadow Copy Service (RVSS) Role: Windows Hyper-V SQL Server Windows Ancillary Function Driver for WinSock Windows App Store Windows Autopilot Windows Container Isolation FS Filter Driver	Windows Container Manager Service Windows Defender Windows Encrypting File System (EFS) Windows File History Service Windows Installer Windows iSCSI Windows Kerberos Windows Kernel Windows LDAP - Lightweight Directory Access Protocol Windows Local Security Authority Subsystem Service Windows Media Windows Network Address Translation (NAT) Windows Network File System Windows PowerShell Windows SMB
Officially Acknowledged by the Vendor	Yes	
Patch/ Workaround Released	Yes	
Reference	https://msrc.microsoft.com/update-guide/releaseNote/2022-Jun	

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.