Advisory Alert

Alert Number: AAA20230410 **Date:** April 10, 2023

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Cisco	**Critical**	Multiple Vulnerabilities
IBM	**High**	Denial of service Vulnerability
Cisco	**High**, **Medium**	Multiple Vulnerabilities

Description

Affected Product	**Cisco**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-20812, CVE-2022-20813)
Description	Cisco has released security updates addressing multiple vulnerabilities that exists in the API and in the web-based management interface of Cisco Expressway Series and Cisco TelePresence Video Communication Server (VCS). **CVE-2022-20812-** A vulnerability exists because of the insufficient input validation of user supplied command arguments. A remote attacker with Administrator read-write privileges can submit the crafted input to the affected command leading to arbitrary file overwrite on the underlying operating system as the root user. **CVE-2022-20813 –** A null byte poisoning vulnerability that exists because of the improper certificate validation. An attacker can exploit this vulnerability by using a man in the middle attack to monitor the traffic and using a crafted certificate, the attacker can intercept traffic in clear text or alter the contents of the traffic**.** Cisco highly recommends to apply necessary security fixes at earliest to avoid issues.
Affected Products	Cisco Expressway Series and Cisco TelePresence VCS Release 14.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-expressway-overwrite-3buqW8LH

Affected Product	**IBM**
Severity	**High**
Affected Vulnerability	Denial of service Vulnerability (CVE-2023-24998)
Description	IBM has released security updates addressing a Denial of service vulnerability that exists in their IBM WebSphere. By sending a specially-crafted request with a series of uploads, a remote attacker can execute a denial of service condition due to not limiting the number of request parts to be processed in the file upload function of Apache Commons FileUpload and Tomcat. IBM recommends to apply necessary security fixes at earliest to avoid issues.
Affected Products	IBM WebSphere Hybrid Edition version 5.1 IBM WebSphere Application Server Liberty versions 17.0.0.3 - 23.0.0.3 IBM WebSphere Application Server version 9.0 IBM WebSphere Application Server version 8.5
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/6982047 https://www.ibm.com/support/pages/node/6982141

Affected Product	**Cisco**
Severity	**High,** **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-20102, CVE-2023-20051, CVE-2023-20069)
Description	Cisco has release security updates addressing multiple vulnerabilities that exist in their products. If exploited these vulnerabilities could lead to Cross-Site Scripting, Denial of service and Remote Code Execution. **CVE-2023-20102-** A Remote Code Execution Vulnerability exists due to insufficient sanitization of user-provided data that is parsed into system memory in the web-based management interface of Cisco Secure Network Analytics. A successful exploitation of this vulnerability could allow an attacker to execute arbitrary code on the underlying operating system by sending a crafted HTTP request to an affected device. **CVE-2023-20051-** A Denial of Service Vulnerability exists due to improperly handling malformed packets in the Vector Packet Processor of Cisco Packet Data Network Gateway. A successful exploitation of this vulnerability could allow an unauthenticated, remote attacker to stop ICMP traffic over an IPsec connection by sending a malformed Encapsulating Security Payload. **CVE-2023-20069-** A Cross-Site Scripting Vulnerability exists due to insufficient validation of user-supplied input in the web-based management interface of Cisco Prime Infrastructure and Cisco Evolved Programmable Network. A successful exploitation of this vulnerability could allow an authenticated, remote attacker to conduct a stored cross-site scripting (XSS) attack by persuading a user of an affected interface to view a page containing malicious HTML or script content. Cisco recommends to apply necessary security fixes at earliest to avoid issues.
Affected Products	Cisco Secure Network Analytics Release 7.4.1 and earlier Cisco PGW Release Earlier than 21.27 Cisco Prime Infrastructure Release Earlier than 3.10.3 Cisco EPN Manager Release Earlier than 7.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-stealthsmc-rce-sfNBPjcS https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cisco-pdng-dos-KmzwEy2Q https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cisco-pi-epnm-xss-mZShH2J

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.