Advisory Alert

Alert Number: AAA20221110 **Date:** November 10, 2022

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
IBM	**Critical**	Multiple Vulnerabilities
SAP	**Critical**	Multiple Vulnerabilities
Cisco	**High, Medium**	Multiple Vulnerabilities
Debian	**High, Medium**	Multiple Vulnerabilities
Ubuntu	**High, Medium**	Multiple Vulnerabilities
SAP	**High, Medium**	Multiple Vulnerabilities

Description

Affected Product	**IBM**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-29154, CVE-2022-38177, CVE-2022-40674, CVE-2022-2526, CVE-2021-42581, CVE-2022-0536, CVE-2022-0155, CVE-2022-2596, CVE-2020-15168, CVE-2022-0235, CVE-2020-7753, CVE-2020-28500, CVE-2021-23337, CVE-2019-10744, CVE-2020-8203, CVE-2021-43307, CVE-2021-3795)
Description	IBM has released security updates addressing multiple critical vulnerabilities that exist in IBM QRadar SIEM. Exploitation of the most severe vulnerabilities cause denial of service, arbitrary code execution and information disclosure. IBM highly recommends to apply the necessary security updates at earliest to avoid issues.
Affected Products	IBM QRadar Network Packet Capture 7.4.0 – 7.4.3 Fix Pack 5 IBM QRadar Network Packet Capture 7.5.0 – 7.5.0 Update Package 2 IBM QRadar Assistant 1.0.0 – 3.5.2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/6838295 https://www.ibm.com/support/pages/node/6838293

Affected Product	**SAP**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-41203, CVE-2021-20223, CVE-2022-35737, CVE-2022-41204)
Description	SAP has released security updates for November 2022 addressing multiple critical Vulnerabilities that exist in their products. Successful exploitation of these vulnerabilities can lead to deserialization of untrusted data, array-bounds overflow, arbitrary code injection, SAP highly recommends to apply the necessary security updates at earliest to avoid issues.
Affected Products	SAP BusinessObjects Business Intelligence Platform (Central Management Console and BI Launchpad), Versions -4.2, 4.3 SAPUI5 CLIENT RUNTIME, Versions –600, 700, 800, 900, 1000 SAPUI5, Versions –754, 755, 756, 757 SAP Commerce, Versions -1905, 2005, 2105, 2011, 2205
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://dam.sap.com/mac/app/e/pdf/preview/embed/ucQrx6G?ltr=a&rc=100

Affected Product	**Cisco**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-20927, CVE-2022-20826, CVE-2022-20946, CVE-2022-20918, CVE-2022-20854, CVE-2022-20922, CVE-2022-20943, CVE-2022-20950, CVE-2022-20940, CVE-2022-20831, CVE-2022-20832, CVE-2022-20833, CVE-2022-20834, CVE-2022-20835, CVE-2022-20836, CVE-2022-20838, CVE-2022-20839, CVE-2022-20840, CVE-2022-20843, CVE-2022-20872, CVE-2022-20905, CVE-2022-20932, CVE-2022-20935, CVE-2022-20936, CVE-2022-20941, CVE-2022-20925, CVE-2022-20926, CVE-2022-20928)
Description	Cisco has released security updates addressing multiple vulnerabilities that exist in their products. Attackers can exploit these vulnerabilities to cause denial of service, arbitrary code execution, information disclosure and TLS session decryption. Cisco highly recommends to apply the necessary security updates at earliest to avoid issues.
Affected Products	Cisco ASA Software Release 9.17, 9.18 Cisco FTD Software Release 7.1, 7.2 Cisco FirePOWER Software Release 7.0 Cisco Cyber Vision Release 3.x, 4.0, 4.1 Cisco Meraki MX Security Appliances Release MX15 and earlier, MX16, MX17, MX18 Snort 3.x Cisco FTD Software 7.2.0 or 7.2.0.1 that had the Snort 3 detection engine configured with an SIP inspection policy. Cisco products running a vulnerable release of Cisco ASA Software or Cisco FTD Software • ASA 5500-X Series • Firepower 4100 Series • Firepower 9300 Series Cisco FTD Software releases 6.3.0 and later
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ssl-client-dos-cCrQPkA https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-fw3100-secure-boot-5M8mUh26 https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ftd-gre-dos-hmedHQPM https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-fmcsfr-snmp-access-6gqgtJ4S https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-fmc-dos-OwEunWJN https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-snort-smb-3nfhJtr https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ftdsnort3sip-dos-A4cHeArC https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ftd-tls-bb-rCgtmY2 https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-fmc-xss-LATZYzxs https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-fmc-info-disc-UghNRRhP https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-fmc-cmd-inj-Z3B5MY35 https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asa-ftd-vp-authz-N2GckjN6

Affected Product	**Debian**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-42799, CVE-2022-42823, CVE-2022-42824, CVE-2021-42387, CVE-2021-42388, CVE-2021-43304, CVE-2021-43305)
Description	Debian has released security updates addressing multiple vulnerabilities that exist in their products. Attackers could exploit these vulnerabilities to cause interface spoofing, arbitrary code execution, information disclosure and buffer overflow. Debian highly recommends to apply the necessary security updates at earliest to avoid issues.
Affected Products	webkit2gtk (PTS) 2.36.4-1~deb10u1 wpewebkit (PTS) 2.36.7-1~deb11u1 clickhouse (PTS) 18.16.1+ds-4 clickhouse (PTS) 18.16.1+ds-7.2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.debian.org/lts/security/2022/dla-3183 https://www.debian.org/lts/security/2022/dla-3176

Affected Product	**Ubuntu**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-2869, CVE-2022-3627, CVE-2022-3599, CVE-2022-2519, CVE-2022-3598, CVE-2022-34526, CVE-2022-2867, CVE-2022-2868, CVE-2022-2520, CVE-2022-2521, CVE-2022-3570, CVE-2022-2953, CVE-2022-3626, CVE-2022-44638, CVE-2022-31630, CVE-2022-37454, CVE-2022-31628, CVE-2022-31629, CVE-2022-21618, CVE-2022-21626, CVE-2022-39399, CVE-2022-21628, CVE-2022-21619, CVE-2022-21624, CVE-2021-24031, CVE-2021-24032)
Description	Ubuntu has released security updates addressing multiple vulnerabilities that exist in their products. Attackers can exploit these vulnerabilities to cause denial of service, arbitrary code execution, information disclosure and server crash. Ubuntu highly recommends to apply the necessary security updates at earliest to avoid issues.
Affected Products	Ubuntu 22– versions prior to Ubuntu 22.1 Ubuntu 20– versions prior to Ubuntu 20.04 Ubuntu 18– versions prior to Ubuntu 18.04 Ubuntu 16– versions prior to Ubuntu 16.04 Ubuntu 14– versions prior to Ubuntu 14.04
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://ubuntu.com/security/notices/USN-5714-1 https://ubuntu.com/security/notices/USN-5718-1 https://ubuntu.com/security/notices/USN-5717-1 https://ubuntu.com/security/notices/USN-5719-1 https://ubuntu.com/security/notices/USN-5720-1

Affected Product	**SAP**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-41214, CVE-2022-41212, CVE-2022-35291, CVE-2022-41211, CVE-2022-41259, CVE-2022-41258, CVE-2022-41260, CVE-2022-41208,CVE-2022-41207, CVE-2022-41205, CVE-2022-41215)
Description	SAP has released security updates for November 2022 addressing multiple vulnerabilities that exist in their products. Attackers can exploit these vulnerabilities to cause application compromise, arbitrary read and write, Stack-based buffer overflow, server crash and information disclosure, SAP highly recommends to apply the necessary security updates at earliest to avoid issues.
Affected Products	SAP NetWeaver Application Server ABAP and ABAP Platform,Versions-700, 731, 804, 740, 750, 789 SAP SuccessFactors attachmentAPIfor Mobile Application(Android &iOS), Versions -<8.1.2High8.1 SAP 3D Visual Enterprise Author,Version -9.0 SAP 3D Visual Enterprise Viewer,Version -9.0 SAP SQL Anywhere, Version -17.0 SAP Financial Consolidation, Version -1010 SAP Biller Direct, Versions-635, 750 SAP GUI for Windows, Version –7.70 SAP NetWeaver ABAP Server and ABAP Platform, Versions-700, 731, 740, 750, 789
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://dam.sap.com/mac/app/e/pdf/preview/embed/ucQrx6G?ltr=a&rc=100

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.