Advisory Alert

Alert Number: **AAA20231212** **Date:** **December 12, 2023**

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
SAP	**Critical**	Multiple Vulnerabilities
Barracuda	**Critical**	Security Update
Dell	**High**	Multiple Vulnerabilities
IBM	**High** , **Medium**	Multiple Vulnerabilities
QNAP	**High** , **Medium**	Multiple Vulnerabilities
Ubuntu	**High** , **Medium**	Multiple Vulnerabilities
SAP	**High**, **Medium**, **Low**	Multiple Vulnerabilities

Description

Affected Product	**SAP**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-49583, CVE-2023-50422, CVE-2023-50423, CVE-2023-50424, CVE-2023-36922)
Description	SAP has released a security update addressing multiple critical vulnerabilities exist in their products.by exploiting, these vulnerabilities could lead to Privilege escalation and OS command injection SAP highly recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	SAP Business Client Versions: 6.5, 7.0, 7.70 SAP Business Technology Platform (BTP) Security Services Integration Libraries- @sap/xssec Versions below 3.6.0 cloud-security-services-integration-library Versions below 2.17.0 & 3.0.0 to 3.3.0 sap-xssec Versions below 4.0.1 github.com/sap/cloud-security-client-go Versions below 0.17.0 SAP ECC and SAP S/4HANA (IS-OIL) Versions: 600, 602, 603, 604, 605, 606, 617, 618, 800, 802, 803, 804, 805, 806, 807
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	**Barracuda**
Severity	**Critical**
Affected Vulnerability	Security Update
Description	Barracuda has released a security update addressing multiple critical security flaws exist in File Upload Protection and JSON Security features of Barracuda Web Application Firewall.by exploiting, these vulnerabilities could bypass Barracuda WAF features. Barracuda highly recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	Barracuda Web Application Firewall Firmware 11.X Barracuda Web Application Firewall Firmware 12.0 Barracuda Web Application Firewall Firmware 12.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://campus.barracuda.com/product/webapplicationfirewall/doc/102888530/security-advisory/

Affected Product	**Dell**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-23583, CVE-2023-5870,CVE-2023-5869,CVE-2023-5868, CVE-2023-5345,CVE-2023-5178,CVE-2023-4921,CVE-2023-4881,CVE-2023-4813,CVE-2023-4693,CVE-2023-4692,CVE-2023-46813,CVE-2023-4641,CVE-2023-4623,CVE-2023-46228,CVE-2023-4622,CVE-2023-45853,CVE-2023-4563,CVE-2023-44487,CVE-2023-4389,CVE-2023-43804,CVE-2023-42754,CVE-2023-42753,CVE-2023-42669,CVE-2023-4155,CVE-2023-4154,CVE-2023-41080,CVE-2023-4091,CVE-2023-4039,CVE-2023-4015,CVE-2023-39194,CVE-2023-39193,CVE-2023-39192,CVE-2023-39189,CVE-2023-38546,CVE-2023-38545,CVE-2023-3777,CVE-2023-34324,CVE-2023-34059,CVE-2023-34058,CVE-2023-31085,CVE-2023-28756,CVE-2023-28755,CVE-2023-23559,CVE-2023-22081,CVE-2023-2177,CVE-2023-2163,CVE-2023-1859,CVE-2023-1829,CVE-2023-1206,CVE-2023-1192,CVE-2022-37026,CVE-2021-41817,CVE-2021-33621)
Description	Dell has released a security update addressing multiple vulnerabilities exist in their products.by exploiting, these vulnerabilities could lead to denial of service, privilege escalation, information disclosure, use-after-free Dell recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	Dell EMC VxRail Appliance 8.0.x versions prior to 8.0.201
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000220369/dsa-2023-465-security-update-for-dell-vxrail-multiple-third-party-component-vulnerabilities-8-0-201

Affected Product	**IBM**
Severity	**High , Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-45166, CVE-2023-45174, CVE-2023-45170, CVE-2023-49877, CVE-2023-49878)
Description	IBM has released a security update addressing multiple vulnerabilities exist in their products.by exploiting, these vulnerabilities could lead to denial of service, privilege escalation and information disclosure IBM recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	IBM System Storage Virtualization Engine TS7700 3957-VED, 3948-VED, 3957-VEC AIX 7.2, 7.3 VIOS 3.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7092383 https://www.ibm.com/support/pages/node/7095022

Affected Product	**QNAP**
Severity	**High , Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-4154, CVE-2023-42669, CVE-2023-4091, CVE-2023-3961, CVE-2023-42670, CVE-2023-32968, CVE-2023-32975, CVE-2023-47565, CVE-2023-23372)
Description	QNAP has released a security update addressing multiple vulnerabilities exist in their products.by exploiting, these vulnerabilities could lead to OS command injection, Code execution, Sensitive information disclosure QNAP recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	QTS 4.5.x QTS 5.0.x QTS 5.1.x QuTS hero h4.5.x QuTS hero h5.0.x QuTS hero h5.1.x QVR Firmware 4.x
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.qnap.com/en/security-advisory/qsa-23-20 https://www.qnap.com/en/security-advisory/qsa-23-07 https://www.qnap.com/en/security-advisory/qsa-23-48 https://www.qnap.com/en/security-advisory/qsa-23-40

Affected Product	**Ubuntu**
Severity	**High , Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-39194, CVE-2023-39193, CVE-2023-5178, CVE-2023-6176, CVE-2023-39192, CVE-2023-37453, CVE-2023-5717, CVE-2023-39189, CVE-2023-42754, CVE-2023-3006)
Description	Ubuntu has released a security update addressing multiple vulnerabilities exist in their products.by exploiting, these vulnerabilities could lead to denial of service, sensitive information disclosure and arbitrary code execution. Ubuntu recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	Ubuntu 20.04 LTS Ubuntu 18.04 ESM
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://ubuntu.com/security/notices/USN-6548-1

Affected Product	**SAP**
Severity	**High, Medium, Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-42481, CVE-2023-42478, CVE-2023-49580, CVE-2023-6542, CVE-2023-42476, CVE-2023-49587, CVE-2023-42479, CVE-2023-49577, CVE-2021-23413, CVE-2023-49584, CVE-2023-49581, CVE-2023-49058, CVE-2023-49578)
Description	SAP has released a security update addressing multiple vulnerabilities exist in their products.by exploiting, these vulnerabilities could lead to Improper Access Control, Cross site scripting, Information disclosure, Command Injection SAP recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	SAP Commerce Cloud - Version 8.1 Business Objects BI Platform - Versions 420, 430 SAP GUI for Windows and SAP GUI for Java - Versions SAP_BASIS 755, SAP_BASIS 756, SAP_BASIS 757, SAP_BASIS 758 SAP EMARSYS SDK ANDROID - Version 3.6.2 SAP BusinessObjects Web Intelligence - Version 420 SAP Solution Manager - Version 720 SAP Biller Direct - Versions 635, 750 SAP HCM (SMART PAYE solution) - Versions S4HCMCIE 100, SAP_HRCIE 600, SAP_HRCIE 604, SAP_HRCIE 608 SAPUI5 - Versions SAP_UI 750, SAP_UI 753, SAP_UI 754, SAP_UI 755, SAP_UI 756, UI_700 200 SAP Fiori Launchpad - Versions SAP_UI 750, SAP_UI 754, SAP_UI 755, SAP_UI 756, SAP_UI 757, SAP_UI 758, UI_700 200, SAP_BASIS 793 SAP NetWeaver Application Server ABAP and ABAP Platform - Versions SAP_BASIS 700, SAP_BASIS731, SAP_BASIS740, SAP_BASIS750 SAP Master Data Governance - Versions 731, 732, 746, 747, 748, 749, 800, 751,752,801,802, 803, 804, 805, 806, 807, 808 SAP Cloud Connector - Version 2.0
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.