Advisory Alert

Alert Number: AAA20221118 **Date:** November 18, 2022

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
HP	**High**	Remote Authentication Bypass Vulnerability
SUSE	**High**	Multiple Vulnerabilities
Ubuntu	**High**, Medium	Multiple Vulnerabilities
Debian	**High**, Medium	Multiple Vulnerabilities

Description

Affected Product	**HP**
Severity	**High**
Affected Vulnerability	Remote Authentication Bypass Vulnerability (CVE-2022-37932)
Description	HP has released a security update to address a remote authentication bypass vulnerability that exist in their enterprise OfficeConnect 1820, 1850, and 1920S Network switches. A remote attacker can exploit this vulnerability to cause authentication bypass. HP recommends to apply the necessary patch updates at your earliest to avoid issues
Affected Products	HPE OfficeConnect 1820 8G Switch J9979A - Prior to PT.02.14 HPE OfficeConnect 1820 8G PoE+ (65W) Switch J9982A - Prior to PT.02.14 HPE OfficeConnect 1820 24G Switch J9980A - Prior to PT.02.14 HPE OfficeConnect 1820 24G PoE+ (185W) Switch J9983A - Prior to PT.02.14 HPE OfficeConnect 1820 48G Switch J9981A - Prior to PT.02.14 HPE OfficeConnect 1820 48G PoE+ (370W) Switch J9984A - Prior to PT.02.14 HPE OfficeConnect 1850 24G 2XGT PoE+ 185W Switch - Prior to PC.01.22 HPE OfficeConnect 1850 24G 2XGT Switch - Prior to PC.01.22 HPE OfficeConnect 1850 48G 4XGT PoE+ 370W Switch - Prior to PC.01.22 HPE OfficeConnect 1850 48G 4XGT Switch - Prior to PC.01.22 HPE OfficeConnect 1850 6XGT and 2XGT/SPF+ Switch - Prior to PO.01.21 HPE OfficeConnect 1920S 24G 2SFP PoE+ 370W Switch - Prior to PD.02.22 HPE OfficeConnect 1920S 24G 2SFP PPoE+ 185W Switch - Prior to PD.02.22 HPE OfficeConnect 1920S 24G 2SFP Switch - Prior to PD.02.22 HPE OfficeConnect 1920S 48G 4SFP PPoE+ 370W Switch - Prior to PD.02.22 HPE OfficeConnect 1920S 48G 4SFP Switch - Prior to PD.02.22 HPE OfficeConnect 1920S 8G PPoE+ 65W Switch - Prior to PD.02.22 HPE OfficeConnect 1920S 8G Switch - Prior to PD.02.22
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbnw04383en_us

Affected Product	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities(CVE-2018-10903, CVE-2021-28689, CVE-2022-33746, CVE-2022-33748, CVE-2022-42309, CVE-2022-42310, CVE-2022-42311, CVE-2022-42312, CVE-2022-42313, CVE-2022-42314, CVE-2022-42315, CVE-2022-42316, CVE-2022-42317, CVE-2022-42318, CVE-2022-42320, CVE-2022-42321, CVE-2022-42322, CVE-2022-42323, CVE-2021-4037, CVE-2022-2153, CVE-2022-2964, CVE-2022-2978, CVE-2022-3176, CVE-2022-3424, CVE-2022-3521, CVE-2022-3524, CVE-2022-3535, CVE-2022-3542, CVE-2022-3545, CVE-2022-3565, CVE-2022-3577, CVE-2022-3586, CVE-2022-3594, CVE-2022-3621, CVE-2022-3625, CVE-2022-3629, CVE-2022-3640, CVE-2022-3646, CVE-2022-3649, CVE-2022-39189, CVE-2022-42703, CVE-2022-43750, CVE-2022-45403, CVE-2022-45404, CVE-2022-45405, CVE-2022-45406, CVE-2022-45408, CVE-2022-45409, CVE-2022-45410, CVE-2022-45411, CVE-2022-45412, CVE-2022-45416, CVE-2022-45418, CVE-2022-45420, CVE-2022-45421)
Description	SUSE has released security updates addressing multiple vulnerabilities that exists in their products. Successful exploitation of the most severe vulnerabilities could cause cryptographic key leakage, denial of service, gusts accessing Xenstore nodes of the deleted domains, arbitrary xen node creation, unwanted file creation on the XFS file system, create a race condition, and memory leakage. SUSE recommends to apply the necessary updates at your earliest to avoid issues
Affected Products	openSUSE Leap 15.3, 15.4 openSUSE Leap Micro 5.2 SUSE Enterprise Storage 7, 7.1 SUSE Linux Enterprise Desktop 15-SP3, 15-SP4 SUSE Linux Enterprise High Availability 15-SP3 SUSE Linux Enterprise High Performance Computing SUSE Linux Enterprise High Performance Computing 15-SP2-ESPOS, 15-SP2-LTSS, 15-SP3, 15-SP4 SUSE Linux Enterprise Micro 5.1, 5.2 SUSE Linux Enterprise Module for Basesystem 15-SP3 SUSE Linux Enterprise Module for Desktop Applications 15-SP3, 15-SP4 SUSE Linux Enterprise Module for Development Tools 15-SP3 SUSE Linux Enterprise Module for Legacy Software 15-SP3 SUSE Linux Enterprise Module for Live Patching 15-SP3 SUSE Linux Enterprise Module for Python2 15-SP3 SUSE Linux Enterprise Server SUSE Linux Enterprise Server 12-SP2-BCL, 15-SP2-BCL, 15-SP2-LTSS, 15-SP3, 15-SP4 SUSE Linux Enterprise Server for SAP 15-SP2 SUSE Linux Enterprise Server for SAP Applications, 15-SP3, 15-SP4 SUSE Linux Enterprise Workstation Extension 15-SP3 SUSE Manager Proxy 4.1, 4.2, 4.3 SUSE Manager Retail Branch Server 4.1, 4.2, 4.3 SUSE Manager Server 4.1, 4.2, 4.3
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.suse.com/support/update/announcement/2022/suse-su-20224044-1/ https://www.suse.com/support/update/announcement/2022/suse-su-20224051-1/ https://www.suse.com/support/update/announcement/2022/suse-su-20224053-1/ https://www.suse.com/support/update/announcement/2022/suse-su-20224058-1/

Affected Product	**Ubuntu**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-3635, CVE-2022-29901, CVE-2022-39188, CVE-2022-2978, CVE-2022-2153, CVE-2022-42719, CVE-2022-3625, CVE-2022-3028, CVE-2022-20422, CVE-2022-42703, CVE-2022-41222, CVE-2022-40768, CVE-2022-2905, CVE-2022-39190, CVE-2022-43680, CVE-2022-40674, CVE-2022-42823, CVE-2022-32923, CVE-2022-32888, CVE-2022-42824, CVE-2022-42799, CVE-2022-41974, CVE-2022-41973, CVE-2022-3204, CVE-2022-39260)
Description	Ubuntu has released security updates addressing multiple vulnerabilities that exists in their products and packages. Successful exploitation of these vulnerabilities could cause denial of service, arbitrary code execution and sensitive data exposure. Ubuntu recommends to apply the necessary updates at your earliest to avoid issues
Affected Products	Ubuntu 20.04 LTS Ubuntu 18.04 LTS Ubuntu 22.04 Ubuntu 20.04 Ubuntu 18.04 Ubuntu 22.10 Ubuntu 16.04
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://ubuntu.com/security/notices/USN-5728-1 https://ubuntu.com/security/notices/USN-5729-1 https://ubuntu.com/security/notices/USN-5638-2 https://ubuntu.com/security/notices/USN-5730-1 https://ubuntu.com/security/notices/USN-5731-1 https://ubuntu.com/security/notices/USN-5732-1 https://ubuntu.com/security/notices/USN-5686-2

Affected Product	**Debian**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2021-45452, CVE-2022-22818, CVE-2022-23833, CVE-2022-42902, CVE-2022-21797, CVE-2022-39286, CVE-2021-30130, CVE-2022-45403, CVE-2022-45404, CVE-2022-45405, CVE-2022-45406, CVE-2022-45408, CVE-2022-45409, CVE-2022-45410, CVE-2022-45411, CVE-2022-45412, CVE-2022-45416, CVE-2022-45418, CVE-2022-45420, CVE-2022-45421)
Description	Debian has released security updates addressing multiple vulnerabilities that exists the packages that is used by their products. Successful exploitation of these vulnerabilities could cause directory traversal, cross site scripting (XSS), creating an infinite loop, remote code execution, arbitrary code execution and spoofing bypass. Debian recommends to apply the necessary updates at your earliest to avoid issues
Affected Products	Debian 10 Buster, versions before 1:1.11.29-1+deb10u4 Debian 10 Buster, versions before 2019.01-5+deb10u1 Debian 10 Buster, versions before 0.13.0-2+deb10u1 Debian 10 Buster, versions before 4.4.0-2+deb10u1. Debian 10 Buster, versions before 1.0.19-3~deb10u1. Debian 10 Buster, versions before 2.0.30-2~deb10u1. Debian 10 buster, versions before 1:102.5.0-1~deb10u1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.debian.org/lts/security/2022/dla-3191 https://www.debian.org/lts/security/2022/dla-3192 https://www.debian.org/lts/security/2022/dla-3193 https://www.debian.org/lts/security/2022/dla-3195 https://www.debian.org/lts/security/2022/dla-3197 https://www.debian.org/lts/security/2022/dla-3198 https://www.debian.org/lts/security/2022/dla-3196

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.