Advisory Alert

Alert Number: AAA20221121 **Date:** November 21, 2022

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
HP	**High**	Multiple Vulnerabilities
SUSE	**High**	Multiple Vulnerabilities

Description

Affected Product	**HP**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-37931, CVE-2022-33186)
Description	HP has released security update to address multiple vulnerabilities that exist in their products. **CVE-2022-37931 –** A vulnerability that exist in the NetBatch-Plus software that allows unauthorized access to the application**.** **CVE-2022-33186 –** A vulnerability that exist in the HPE SAN switches with vulnerable Brocade Fabric OS (FOS) versions that could allow a remote attacker to bypass authentication and perform unauthorized configuration changes. HP recommends to apply the necessary patch updates at your earliest to avoid issues
Affected Products	Netbatch Plus T9189 T9189L01 - T9189L01^ABY; T9189H01 – T9189H01^ABW HPE SN8000B 4-slot SAN Director Switch - v8.x prior to v8.2.3c1 HPE SN8000B 8-slot SAN Director Switch - v8.x prior to v8.2.3c1 HPE SN8600B 4-slot SAN Director Switch - v9.1.x prior to v9.1.1_01, v9.0.x prior to v9.0.1e1 and v8.x prior to v8.2.3c1 HPE SN8600B 8-slot SAN Director Switch - v9.1.x prior to v9.1.1_01, v9.0.x prior to v9.0.1e1 and v8.x prior to v8.2.3c1 HPE SN8700B 4-slot SAN Director Switch - v9.1.x prior to v9.1.1_01 and v9.0.x prior to v9.0.1e1 HPE SN8700B 8-slot SAN Director Switch - v9.1.x prior to v9.1.1_01 and v9.0.x prior to v9.0.1e1 HPE SN3000B Fibre Channel Switch - v8.x prior to v8.2.3c1 HPE B-series SN3600B Fibre Channel Switch - v9.1.x prior to v9.1.1_01, v9.0.x prior to v9.0.1e1 and v8.x prior to v8.2.3c1 HPE B-series SN6000B Fibre Channel Switch - v8.x prior to v8.2.3c1 HPE B-series SN6500B Fibre Channel Switch - v8.x prior to v8.2.3c1 HPE B-series SN6600B Fibre Channel Switch - v9.1.x prior to v9.1.1_01, v9.0.x prior to v9.0.1e1 and v8.x prior to v8.2.3c1 HPE B-series SN6650B Fibre Channel Switch - v9.1.x prior to v9.1.1_01, v9.0.x prior to v9.0.1e1 and v8.x prior to v8.2.3c1 HPE B-series SN6700B Fibre Channel Switch - v9.1.x prior to v9.1.1_01 and v9.0.x prior to v9.0.1e1 HPE B-series SN6750B Fibre Channel Switch - v9.1.x prior to v9.1.1_01 HPE B-series SN2600B SAN Extension Switch - v9.1.x prior to v9.1.1_01 and v9.0.x prior to v9.0.1e1 HPE B-series SN4000B SAN Extension Switch - v8.x prior to v8.2.3c1 HPE 8/24 SAN Switch - v7.x prior to v7.4.2j1 HPE 8/8 SAN Switch - v7.x prior to v7.4.2j1 HPE 1606 Extension SAN Switch - v7.x prior to v7.4.2j1 Brocade 8Gb SAN Switch for HPE BladeSystem c-Class - v7.x prior to v7.4.2j1 Brocade 16Gb SAN Switch for HPE BladeSystem c-Class - v8.x prior to v8.2.3c1 Brocade 16Gb/12 Fibre Channel SAN Switch Module for HPE Synergy - v8.x prior to v8.2.3c1 Brocade 16Gb/24 Fibre Channel SAN Switch Module for HPE Synergy - v8.x prior to v8.2.3c1 Brocade 32Gb Fibre Channel SAN Switch for HPE Synergy - v9.1.x prior to v9.1.1_01 and v9.0.x prior to v9.0.1e1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbns04388en_us https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbst04384en_us

Affected Product	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities(CVE-2021-33655, CVE-2022-2588, CVE-2022-42722, CVE-2022-1882, CVE-2022-2959, CVE-2020-36557, CVE-2020-36558, CVE-2022-42703, CVE-2022-37035, CVE-2022-42917, CVE-2015-9253, CVE-2017-8923, CVE-2017-9120, CVE-2018-1000222, CVE-2018-12882, CVE-2018-14851, CVE-2018-17082, CVE-2018-19935, CVE-2018-20783, CVE-2019-11034, CVE-2019-11035 , CVE-2019-11036, CVE-2019-11039, CVE-2019-11040, CVE-2019-11041, CVE-2019-11042, CVE-2019-11043, CVE-2019-11045, CVE-2019-11046, CVE-2019-11047, CVE-2019-11048, CVE-2019-11050, CVE-2019-9020, CVE-2019-9021, CVE-2019-9022, CVE-2019-9023, CVE-2019-9024, CVE-2019-9637, CVE-2019-9638, CVE-2019-9640, CVE-2019-9641, CVE-2019-9675, CVE-2020-7059, CVE-2020-7060, CVE-2020-7062, CVE-2020-7063, CVE-2020-7064, CVE-2020-7066, CVE-2020-7069, CVE-2020-7070, CVE-2020-7071, CVE-2021-21702, CVE-2021-21703, CVE-2021-21704, CVE-2021-21705, CVE-2021-21707, CVE-2022-31625, CVE-2022-31626, CVE-2022-31628, CVE-2022-31629, CVE-2022-37454, CVE-2017-8923, CVE-2021-21706, CVE-2021-21708, CVE-2022-31630, CVE-2020-7068, CVE-2022-42919, CVE-2022-45061, CVE-2022-2153, CVE-2022-28748, CVE-2022-2964, CVE-2022-2978, CVE-2022-3169, CVE-2022-33981, CVE-2022-3424, CVE-2022-3435, CVE-2022-3521, CVE-2022-3524, CVE-2022-3526, CVE-2022-3535, CVE-2022-3542, CVE-2022-3545, CVE-2022-3565, CVE-2022-3577, CVE-2022-3586, CVE-2022-3594, CVE-2022-3619, CVE-2022-3621, CVE-2022-3625, CVE-2022-3628, CVE-2022-3629, CVE-2022-3633, CVE-2022-3640, CVE-2022-3646, CVE-2022-3649, CVE-2022-40476, CVE-2022-40768, CVE-2022-43750, CVE-2019-12387, CVE-2020-10108, CVE-2022-21712, CVE-2022-39348, CVE-2022-43995, CVE-2018-20846, CVE-2018-21010, CVE-2020-27824, CVE-2020-27842, CVE-2020-27843, CVE-2020-27845,CVE-2022-43548)
Description	SUSE has released security updates addressing multiple vulnerabilities that exists in their products and packages. Successful exploitation of the most severe vulnerabilities could cause out of bounds write, create use after free condition, buffer overflow, cookie manipulation, privilege escalation, kernel memory leak, denial of service, and DNS rebinding. SUSE recommends to apply the necessary updates at your earliest to avoid issues
Affected Products	HPE Helion Openstack 8 openSUSE Leap 15.3, 15.4 openSUSE Leap Micro 5.2 SUSE CaaS Platform 4.0 SUSE Enterprise Storage 6, 7, 7.1 SUSE Linux Enterprise Desktop 15-SP3, 15-SP4 SUSE Linux Enterprise High Availability 15-SP4 SUSE Linux Enterprise High Performance Computing SUSE Linux Enterprise High Performance Computing 12, 15, 15-ESPOS, 15-LTSS, 15-SP1, 15-SP1-ESPOS, 15-SP1-LTSS, 15-SP2, 15-SP2-ESPOS, 15-SP2-LTSS, 15-SP3, 15-SP4 SUSE Linux Enterprise Live Patching 12-SP4, 12-SP5 SUSE Linux Enterprise Micro 5.1, 5.2, 5.3 SUSE Linux Enterprise Module for Basesystem 15-SP3, 15-SP4 SUSE Linux Enterprise Module for Desktop Applications 15-SP3, 15-SP4 SUSE Linux Enterprise Module for Development Tools 15-SP3, 15-SP4 SUSE Linux Enterprise Module for Legacy Software 15-SP4 SUSE Linux Enterprise Module for Live Patching 15, 15-SP1, 15-SP2, 15-SP3, 15-SP4 SUSE Linux Enterprise Module for Packagehub Subpackages 15-SP3 SUSE Linux Enterprise Module for Server Applications 15-SP3, 15-SP4 SUSE Linux Enterprise Module for Web Scripting 12, 15-SP3 SUSE Linux Enterprise Server SUSE Linux Enterprise Server 12, 12-SP3, 12-SP4, 12-SP5 SUSE Linux Enterprise Server 15, 15-LTSS, 15-SP1, 15-SP1-BCL, 15-SP1-LTSS, 15-SP2, 15-SP2-BCL, 15-SP2-LTSS, 15-SP3, 15-SP4 SUSE Linux Enterprise Server for SAP 15, 15-SP1, 15-SP2 SUSE Linux Enterprise Server for SAP Applications 12, 12-SP3, 12-SP4, 12-SP5 SUSE Linux Enterprise Server for SAP Applications 15, 15-SP1, 15-SP2, 15-SP3, 15-SP4 SUSE Linux Enterprise Software Development Kit 12-SP5 SUSE Linux Enterprise Workstation Extension 15-SP4 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 SUSE OpenStack Cloud 8, 9 SUSE OpenStack Cloud Crowbar 8, 9
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.suse.com/support/update/announcement/2022/suse-su-20224100-1/ https://www.suse.com/support/update/announcement/2022/suse-su-20224113-1/ https://www.suse.com/support/update/announcement/2022/suse-su-20224112-1/ https://www.suse.com/support/update/announcement/2022/suse-su-20224129-1/ https://www.suse.com/support/update/announcement/2022/suse-su-20224130-1/ https://www.suse.com/support/update/announcement/2022/suse-su-20224067-1/ https://www.suse.com/support/update/announcement/2022/suse-su-20224068-1/ https://www.suse.com/support/update/announcement/2022/suse-su-20224069-1/ https://www.suse.com/support/update/announcement/2022/suse-su-20224071-1/ https://www.suse.com/support/update/announcement/2022/suse-su-20224072-1/ https://www.suse.com/support/update/announcement/2022/suse-su-20224074-1/ https://www.suse.com/support/update/announcement/2022/suse-su-20224077-1/ https://www.suse.com/support/update/announcement/2022/suse-su-20224082-1/ https://www.suse.com/support/update/announcement/2022/suse-su-20224084-1/

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.