Advisory Alert

Alert Number: AAA20240416 **Date:** April 16, 2024

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
HPE	**Critical**	Multiple Vulnerabilities
HPE	**High**	Multiple Vulnerabilities
Netgear	**High**	Authentication Bypass Vulnerability
Red Hat	**High**	Multiple Vulnerabilities
SUSE	**High**	Multiple Vulnerabilities

Description

Affected Product	**HPE**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2021-38578)
Description	HPE has issued security updates addressing multiple vulnerabilities that exist in HPE Superdome Flex and Compute Scale-up servers. These vulnerabilities could be exploited to overwrite SMM memory leading to execution of arbitrary code with privilege elevation. **CVE-2021-38578** - Existing CommBuffer checks in SmmEntryPoint will not catch underflow when computing BufferSize. HPE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	HPE Compute Scale-up Server 3200 - prior to v1.20.128 HPE Superdome Flex 280 Server - prior to v1.70.14 HPE Superdome Flex Server - prior to v3.90.18
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04633en_us

Affected Product	**HPE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-36765, CVE-2024-22440)
Description	HPE has released security updates addressing multiple vulnerabilities that exist in HPE Compute Scale-up Servers. If Exploited, these vulnerabilities could lead to local buffer overflow and sensitive information disclosure. **CVE-2022-36765**- EDK2 is susceptible to a vulnerability in the CreateHob() function, allowing a user to trigger a integer overflow to buffer overflow via a local network. **CVE-2024-22440** - The network communication library in affected systems insufficiently validates HMAC values which might result in a buffer overread. HPE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	HPE Compute Scale-up Server 3200 - prior to v1.20.128
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04632en_us • https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04634en_us

Affected Product	**Netgear**
Severity	**High**
Affected Vulnerability	Authentication Bypass Vulnerability
Description	Netgear has released security updates addressing an Authentication Bypass Vulnerability that exists in RAX series routers. This vulnerability requires an attacker to have your WiFi password or an Ethernet connection to a device on your network to be exploited. Netgear advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Firmware versions prior to 1.0.6.106 in RAX35, RAX38 RAX40 Routers
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://kb.netgear.com/000066096/Security-Advisory-for-Authentication-Bypass-on-Some-Routers-PSV-2023-0166?article=000066096

Affected Product	**Red Hat**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-3611, CVE-2023-3776, CVE-2023-4921, CVE-2023-31436)
Description	Red Hat has released security updates addressing multiple vulnerabilities that exist in Red Hat Linux kernel. If Exploited, these vulnerabilities could lead to out-of-bounds memory write/access and use-after-free conditions. Red Hat advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Red Hat Enterprise Linux Server - Extended Life Cycle Support 6 x86_64 Red Hat Enterprise Linux Server - Extended Life Cycle Support 6 i386 Red Hat Enterprise Linux Server - Extended Life Cycle Support (for IBM z Systems) 6 s390x Red Hat Enterprise Linux Server - Retired Extended Life Cycle Support 6 x86_64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2024:1831

Affected Product	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-52340, CVE-2024-0565, CVE-2024-1085, CVE-2023-42753)
Description	SUSE has released security updates addressing multiple vulnerabilities that exist in their products. If Exploited, these vulnerabilities could lead to out-of-bounds memory read, Denial of Service and use-after-free conditions. SUSE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	openSUSE Leap 15.4 SUSE Linux Enterprise High Performance Computing 15 SP4 SUSE Linux Enterprise Live Patching 15-SP4 SUSE Linux Enterprise Micro 5.3, 5.4 SUSE Linux Enterprise Real Time 15 SP4 SUSE Linux Enterprise Server 15 SP4 SUSE Linux Enterprise Server for SAP Applications 15 SP4
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.suse.com/support/update/announcement/2024/suse-su-20241288-1/ • https://www.suse.com/support/update/announcement/2024/suse-su-20241292-1/ • https://www.suse.com/support/update/announcement/2024/suse-su-20241298-1/ • https://www.suse.com/support/update/announcement/2024/suse-su-20241280-1/

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.