TLP: WHITE

Advisory Alert

Alert Number: AAA20231026 **Date:** October 26, 2023

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Redhat	**High**	HTTP Security Policy Bypass Vulnerability
SonicWall	**High**	Multiple Vulnerabilities
HPE	**High**	Remote Code Execution Vulnerability
Ubuntu	**High**, Medium , Low	Multiple Vulnerabilities
CPanel	Medium	Multiple Vulnerabilities

Description

Affected Product	**Redhat**
Severity	**High**
Affected Vulnerability	HTTP Security Policy Bypass Vulnerability (CVE-2023-4853)
Description	Redhat has released a security update addressing a HTTP Security Policy Bypass vulnerability in their products. Successful exploitation of this vulnerability could allow an attacker to bypass the security policy altogether, resulting in unauthorized endpoint access and possibly a denial of service. Redhat recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	Red Hat JBoss Middleware Text-Only Advisories for MIDDLEWARE 1 x86_64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2023:6112

Affected Product	**SonicWall**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-44219, CVE-2023-44220)
Description	SonicWall has released security update addressing multiple vulnerabilities in their products. **CVE-2023-44219** - A local privilege escalation vulnerability in SonicWall Directory Services Connector Windows MSI client 4.1.21 and earlier versions allows a local low-privileged user to gain system privileges through running the recovery feature. **CVE-2023-44220** - SonicWall NetExtender Windows (32 and 64-bit) client 10.2.336 and earlier versions have a DLL Search Order Hijacking vulnerability in the start-up DLL component. Successful exploitation via a local attacker could result in command execution in the target system. SonicWall recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	SonicWall Directory Services Connector Windows client 4.1.21 and earlier versions. SonicWall NetExtender Windows (32 and 64 bit) 10.2.336 and earlier versions.
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0016 https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0017

Affected Product	**HPE**
Severity	**High**
Affected Vulnerability	Remote Code Execution Vulnerability (CVE-2023-30912)
Description	HPE has released a security update addressing a Remote Code Execution Vulnerability that exist in Hewlett Packard Enterprise OneView Software. HPE recommends to apply the necessary security updates at earliest to avoid issues
Affected Products	HPE OneView - Prior to 8.60.00
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbgn04548en_us

Affected Product	**Ubuntu**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-1206, CVE-2023-4623, CVE-2023-4921, CVE-2023-42755, CVE-2023-42752, CVE-2023-4622, CVE-2023-4881, CVE-2023-42753, CVE-2023-31083, CVE-2023-34319, CVE-2023-3772, CVE-2023-0597)
Description	Ubuntu has released security update addressing multiple vulnerabilities in Ubuntu 16.04. Successful exploitation of these vulnerabilities could lead to Denial of Service, sensitive information disclosure, Arbitrary code Execution. Ubuntu recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	Ubuntu 16.04
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://ubuntu.com/security/notices/USN-6440-3

Affected Product	**CPanel**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-31122, CVE-2023-43622, CVE-2023-45802)
Description	CPanel has released a security update addressing multiple vulnerabilities that affect their products. **CVE-2023-31122** - Out-of-bounds Read vulnerability in mod_macro of Apache HTTP Server.This issue affects Apache HTTP Server: through 2.4.57. **CVE-2023-43622** - An attacker, opening a HTTP/2 connection with an initial window size of 0, was able to block handling of that connection indefinitely in Apache HTTP Server. This could be used to exhaust worker resources in the server, similar to the well known "slow loris" attack pattern. **CVE-2023-45802** - When a HTTP/2 stream was reset (RST frame) by a client, there was a time window were the request's memory resources were not reclaimed immediately. Instead, de-allocation was deferred to connection close. A client could send new requests and resets, keeping the connection busy and open and causing the memory footprint to keep on growing. On connection close, all resources were reclaimed, but the process might run out of memory before that. CPanel recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	cPanel packages for EasyApache 4 with Apache version 2.4.58
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://news.cpanel.com/easyapache4-2023-10-25-maintenance-and-security-release/

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.