Advisory Alert

Alert Number: AAA20221202 **Date:** December 2, 2022

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
HP	**Critical**	Multiple Vulnerabilities
Ubuntu	**High**, **Medium**, **Low**	Multiple Vulnerabilities

Description

Affected Product	**HP**
Severity	**Critical**
Affected Vulnerability	Multiple vulnerabilities (CVE-2022-31813, CVE-2022-30522, CVE-2022-28615, CVE-2022-28614, CVE-2022-26377)
Description	HP has released a security Updates addressing multiple vulnerabilities that exist in the Apache Web Server version-2.4.53.00 running on HP-UX. If exploited these vulnerabilities could cause authentication Restriction Bypass, memory corruption, information disclosure and Server-Side Request Forgery (SSRF). An attacker can exploit these vulnerabilities both locally and remotely. HP highly recommends to apply necessary patch updates at earliest to avoid issues
Affected Products	Apache Web Server version-2.4.53.00 running on HP-UX
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbux04397en_us

Affected Product	**Ubuntu**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple vulnerabilities (CVE-2022-3564, CVE-2022-43945, CVE-2022-3524, CVE-2022-3594, CVE-2022-3566, CVE-2022-3565, CVE-2022-3567, CVE-2022-3621, CVE-2022-42703, CVE-2022-3239 CVE-2022-40768, CVE-2022-3635, CVE-2022-43750, CVE-2022-3649)
Description	Ubuntu has released Security Updates addressing multiple vulnerabilities that effecting the Linux kernel packages. If exploited these vulnerabilities could cause denial of service or execute arbitrary code. Ubuntu recommends to apply necessary security fixes at earliest to avoid issues
Affected Products	Ubuntu 22.10 Ubuntu 22.04 Ubuntu 20.04 Ubuntu 18.04 Ubuntu 16.04 Ubuntu 14.04
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://ubuntu.com/security/notices/USN-5754-1 https://ubuntu.com/security/notices/USN-5755-1 https://ubuntu.com/security/notices/USN-5756-1 https://ubuntu.com/security/notices/USN-5757-1 https://ubuntu.com/security/notices/USN-5757-2 https://ubuntu.com/security/notices/USN-5758-1

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.