Advisory Alert

Alert Number: **AAA20230307** **Date:** **March 7, 2023**

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
SUSE	**High**	Multiple Vulnerabilities
Lenovo	**High**	Multiple Vulnerabilities
HPE	**High, Medium**	Multiple Vulnerabilities
Ubuntu	**High, Medium, Low**	Multiple Vulnerabilities
IBM	**Medium**	Denial of Service Vulnerability

Description

Affected Product	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-3107, CVE-2022-3108, CVE-2022-3564, CVE-2022-36280, CVE-2022-4662, CVE-2022-47929, CVE-2023-0045, CVE-2023-0266, CVE-2023-0590, CVE-2023-23454)
Description	SUSE has released security updates addressing multiple Linux kernel vulnerabilities. Exploitation of these vulnerabilities can lead to null pointer dereference, use-after-free, out of bounds memory access, race condition and denial of service. SUSE recommends to apply necessary security fixes at earliest to avoid issues.
Affected Products	SUSE Linux Enterprise High Performance Computing 12 SP5 SUSE Linux Enterprise Server 12 SP5 SUSE Linux Enterprise Server for SAP Applications 12 SP5
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.suse.com/support/update/announcement/2023/suse-su-20230618-1/

Affected Product	**Lenovo**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-32471, CVE-2022-32475, CVE-2022-32470, CVE-2022-32469, CVE-2022-32477, CVE-2022-32473, CVE-2022-32476, CVE-2022-32472, CVE-2022-32478, CVE-2022-32474, CVE-2022-32953, CVE-2022-32954, CVE-2022-32955, CVE-2022-32952, CVE-2022-32951, CVE-2022-33972)
Description	Lenovo has released security updates addressing multiple vulnerabilities that exist in their BIOSs. Exploitation of these vulnerabilities can lead to information disclosure and privilege escalation. Lenovo recommends to apply necessary security fixes at earliest to avoid issues.
Affected Products	Multiple Products
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.lenovo.com/us/en/product_security/LEN-107840

Affected Product	**HPE**
Severity	**High, Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-36348, CVE-2022-38090, CVE-2022-26837, CVE-2021-0187, CVE-2022-32231, CVE-2022-26343, CVE-2022-36416, CVE-2022-36797)
Description	HPE has released security updates addressing multiple vulnerabilities that exist in their products. Exploitation of these vulnerabilities can lead to privilege escalation, information disclosure. HPE recommends to apply necessary security fixes at earliest to avoid issues.
Affected Products	Multiple Products
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04441en_us https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04408en_us https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04409en_us https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbgn04446en_us

Affected Product	**Ubuntu**
Severity	**High, Medium, Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-42895, CVE-2021-4155, CVE-2022-41858, CVE-2023-0045, CVE-2023-23559, CVE-2022-20566, CVE-2022-3521, CVE-2022-42328, CVE-2022-3640, CVE-2022-3545, CVE-2022-42329, CVE-2023-0461, CVE-2022-3628, CVE-2022-37454, CVE-2022-3623, CVE-2022-4378, CVE-2022-36280, CVE-2022-4139, CVE-2023-0394, CVE-2022-3435, CVE-2023-20938, CVE-2023-23454, CVE-2022-47929, CVE-2022-47520, CVE-2022-3169, CVE-2022-41218, CVE-2023-0266, CVE-2023-23455, CVE-2022-3424, CVE-2022-42896, CVE-2022-41850, CVE-2022-41849, CVE-2022-45934, CVE-2022-3649, CVE-2022-3643, CVE-2023-20928, CVE-2022-43945, CVE-2022-3646, CVE-2022-43750)
Description	Ubuntu has released Security Updates addressing multiple vulnerabilities that exist in their products. Successful exploitation of these vulnerabilities could lead to sensitive information disclosure, denial of service and arbitrary code execution. Ubuntu recommends to apply necessary security fixes at earliest to avoid issues.
Affected Products	Ubuntu 14.04 Ubuntu 16.04 Ubuntu 18.04 Ubuntu 20.04
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://ubuntu.com/security/notices/USN-5926-1 https://ubuntu.com/security/notices/USN-5925-1 https://ubuntu.com/security/notices/USN-5767-3 https://ubuntu.com/security/notices/USN-5917-1 https://ubuntu.com/security/notices/USN-5918-1 https://ubuntu.com/security/notices/USN-5920-1 https://ubuntu.com/security/notices/USN-5919-1

Affected Product	**IBM**
Severity	**Medium**
Affected Vulnerability	Denial of Service Vulnerability (CVE-2023-26281)
Description	IBM has released security updates addressing a denial of service vulnerability that exist in the IBM HTTP Server, which is used by IBM WebSphere Application Server. A remote user can use a specially crafted URL to exploit the vulnerability. IBM recommends to apply necessary security fixes at earliest to avoid issues.
Affected Products	IBM HTTP Server 8.5
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/6958522

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.