Advisory Alert

Alert Number: **AAA20240422** **Date:** **April 22, 2024**

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
HPE	**Critical**	Multiple Vulnerabilities
Palo Alto	**Critical**	Command Injection Vulnerability
HPE	**High**	Multiple Vulnerabilities
Netapp	**High**	Multiple Vulnerabilities
SolarWinds	**High**	SWQL Injection Vulnerability
Ivanti	**High, Medium**	Multiple Vulnerabilities
IBM	**High, Medium**	Multiple Vulnerabilities
Ubuntu	**Medium, Low**	Multiple Vulnerabilities

Description

Affected Product	**HPE**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-20861, CVE-2023-20863, CVE-2023-22006, CVE-2023-22025, CVE-2023-22036, CVE-2023-22041, CVE-2023-22043, CVE-2023-22044, CVE-2023-22045, CVE-2023-22049, CVE-2023-22067, CVE-2023-22081, CVE-2023-25193, CVE-2023-34478, CVE-2023-39410, CVE-2023-39417, CVE-2024-29950, CVE-2024-29951, CVE-2024-29952, CVE-2024-29955, CVE-2024-29956, CVE-2024-29957, CVE-2024-29958, CVE-2024-29959, CVE-2024-29960, CVE-2024-29961, CVE-2024-29962, CVE-2024-29963, CVE-2024-29964, CVE-2024-29965, CVE-2024-29966, CVE-2024-29967, CVE-2024-29968, CVE-2024-29969)
Description	HPE has issued security updates addressing multiple vulnerabilities that exist in HPE B-Series SANnav Management Portal. These vulnerabilities could be exploited locally to cause Arbitrary File Modification, Denial of Service (DoS), Directory Traversal, Disclosure of Information, SQL Injection, Privilege Escalation. HPE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	HPE SANnav Management Software versions Prior to 2.3.0a and 2.3.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbst04631en_us&docLocale=en_US

Affected Product	**Palo Alto**
Severity	**Critical -** Initial release date **12th April 2024 (AAA20240415)**
Affected Vulnerability	Command Injection Vulnerability (CVE-2024-3400)
Description	Palo Alto has released security updates addressing a Command Injection Vulnerability that exists in the GlobalProtect feature of Palo Alto Networks PAN-OS software. If exploited it may allow an unauthenticated attacker to execute arbitrary code with root privileges on the firewall. Palo Alto advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	PAN-OS versions prior to 11.1.0-h3, 11.1.1-h1, 11.1.2-h3 PAN-OS versions prior to 11.0.0-h3, 11.0.1-h4, 11.0.2-h4, 11.0.3-h10, 11.0.4-h1 PAN-OS versions prior to 10.2.0-h3, 10.2.1-h2, 10.2.2-h5, 10.2.3-h13, 10.2.4-h16, 10.2.5-h6, 10.2.6-h3, 10.2.7-h8, 10.2.8-h3, 10.2.9-h1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://security.paloaltonetworks.com/CVE-2024-3400

Affected Product	**HPE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-45229, CVE-2023-45230, CVE-2023-45231, CVE-2023-45232, CVE-2023-45233, CVE-2023-45234, CVE-2023-45235, CVE-2023-45236, CVE-2023-45237)
Description	HPE has released security updates addressing multiple vulnerabilities that exist in HPE Superdome Flex and Compute Scale-up servers. If Exploited remotely, these vulnerabilities could lead to Code Execution, Denial of Service and Disclosure of Information. HPE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	HPE Superdome Flex Server versions Prior to 3.90.18 HPE Superdome Flex 280 Server versions Prior to 1.70.14 HPE Compute Scale-up Server 3200 versions Prior to 1.20.128
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbhf04576en_us&docLocale=en_US

Affected Product	**Netapp**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-51780)
Description	Netapp has released security updates addressing multiple vulnerabilities that exist in NetApp HCI BMC. An issue was discovered in the Linux kernel before 6.6.8. do_vcc_ioctl in net/atm/ioctl.c has a use-after-free because of a vcc_recvmsg race condition. When successfully exploited, this flaw could lead to disclosure of sensitive information, addition or modification of data, or Denial of Service. Netapp advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	NetApp HCI Baseboard Management Controller (BMC) - H300S/H500S/H700S/H410S
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://security.netapp.com/advisory/ntap-20240419-0001/

Affected Product	**SolarWinds**
Severity	**High**
Affected Vulnerability	SWQL Injection Vulnerability (CVE-2024-29001)
Description	SolarWinds has released security updates addressing an SWQL Injection Vulnerability that exists in SolarWinds Platform user interface. This vulnerability requires authentication and user interaction to be exploited. SolarWinds advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Solarwinds Platform 2024.1 and prior versions
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.solarwinds.com/trust-center/security-advisories/cve-2024-29001

Affected Product	**Ivanti**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-21894, CVE-2024-22052, CVE-2024-22053, CVE-2024-22023, CVE-2024-29205)
Description	Ivanti has released security updates addressing multiple vulnerabilities that exist in Ivanti Connect Secure and Policy Secure Gateways. If Exploited, these vulnerabilities could lead to Denial of Service, Arbitrary Code Execution and information disclosure conditions. Ivanti advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	All supported versions 9.x and 22.x of Ivanti Connect Secure and Ivanti Policy Secure gateways
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://forums.ivanti.com/s/article/SA-CVE-2024-21894-Heap-Overflow-CVE-2024-22052-Null-Pointer-Dereference-CVE-2024-22053-Heap-Overflow-and-CVE-2024-22023-XML-entity-expansion-or-XXE-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure-Gateways?language=en_US

Affected Product	**IBM**
Severity	**High, Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2019-10785, CVE-2018-6561, CVE-2020-4051, CVE-2018-15494, CVE-2020-5259, CVE-2024-22329, CVE-2023-45166, CVE-2023-45174, CVE-2023-45170, CVE-2024-3772)
Description	IBM has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to cause Cross-Site Scripting, Arbitrary Code Execution, Server-side request forgery, Privilege Escalation, Denial of Service. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	WebSphere Extreme Scale versions 8.6.1.0 - 8.6.1.6 IBM WebSphere Application Server versions 8.5 and 9.0 IBM WebSphere Application Server Liberty versions 17.0.0.3 - 24.0.0.3 AIX versions 7.2 and 7.3 VIOS version 3.1 App Connect Enterprise Certified Container versions 5.0-lts, 7.1, 7.2, 8.0, 8.1, 8.2, 9.0, 9.1, 9.2, 10.0, 10.1, 11.0 and 11.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.ibm.com/support/pages/node/7148753 • https://www.ibm.com/support/pages/node/7148380 • https://www.ibm.com/support/pages/node/7095022 • https://www.ibm.com/support/pages/node/7148623

Affected Product	**Ubuntu**
Severity	**Medium, Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2019-25162, CVE-2021-46936, CVE-2021-46955, CVE-2021-46966, CVE-2021-46990, CVE-2022-20422, CVE-2023-1382, CVE-2023-1998, CVE-2023-24023, CVE-2023-51043, CVE-2023-51779, CVE-2023-52429, CVE-2023-52445, CVE-2023-52451, CVE-2023-52600, CVE-2023-52603, CVE-2024-23851)
Description	Ubuntu has released security updates addressing multiple vulnerabilities that exist in Ubuntu Linux kernel. These vulnerabilities could be exploited by malicious users to cause Denial of Service, Sensitive Information Disclosure, Arbitrary Code Execution, authentication bypass. Ubuntu advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Ubuntu 23.10 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-6743-1 • https://ubuntu.com/security/notices/USN-6742-1 • https://ubuntu.com/security/notices/USN-6741-1 • https://ubuntu.com/security/notices/USN-6740-1 • https://ubuntu.com/security/notices/USN-6739-1

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.