Advisory Alert

Alert Number: **AAA20230726** **Date:** **July 26, 2023**

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
HPE	**High**	Multiple Vulnerabilities
Ubuntu	**High, Medium**	Multiple Vulnerabilities
NetApp	**Medium**	Sensitive Information Disclosure Vulnerability
VMware	**Medium**	Information Disclosure Vulnerability

Description

Affected Product	**HPE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-25667, CVE-2023-35980, CVE-2023-35981, CVE-2023-35982)
Description	HPE has released a security update addressing multiple vulnerabilities within their products. Exploitation of these vulnerabilities could lead to Arbitrary Code Execution, Disclosure of Sensitive Information, and Buffer Overflow. HPE recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	ArubaOS version 10.4.0.1 and below InstantOS version 8.11.1.0 and below InstantOS version 8.10.0.6 and below InstantOS version 8.6.0.20 and below InstantOS version 6.5.4.24 and below InstantOS version 6.4.4.8-4.2.4.21 and below
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbnw04492en_us

Affected Product	**Ubuntu**
Severity	**High ,Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-35001, CVE-2023-3389, CVE-2023-31248, CVE-2023-32629, CVE-2023-2640, CVE-2023-3269, CVE-2023-3390, CVE-2023-3090, CVE-2023-21106, CVE-2022-47929, CVE-2022-2663, CVE-2022-3635, CVE-2023-2860, CVE-2023-3439, CVE-2023-31436, CVE-2023-30456, CVE-2023-1380)
Description	Ubuntu has released security updates addressing multiple vulnerabilities within their products. If exploited theses vulnerabilities could lead to Denial of service, Sensitive information disclosure and Arbitrary code execution. Ubuntu recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	Ubuntu 23.04 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-6250-1 https://ubuntu.com/security/notices/USN-6249-1 https://ubuntu.com/security/notices/USN-6248-1 https://ubuntu.com/security/notices/USN-6247-1 https://ubuntu.com/security/notices/USN-6246-1 https://ubuntu.com/security/notices/LSN-0096-1

Affected Product	**NetApp**
Severity	**Medium**
Affected Vulnerability	Sensitive Information Disclosure Vulnerability (CVE-2020-23064)
Description	NetApp has released a security update addressing Sensitive Information Disclosure vulnerability within their products. Multiple NetApp products incorporate jQuery. jQuery versions 2.2.0 prior to 3.5.0 are susceptible to a Cross Site Scripting vulnerability that if exploited, could lead to disclosure of sensitive information or addition or modification of data within NetApp. Netapp recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	Management Services for Element Software and NetApp HCI
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://security.netapp.com/advisory/ntap-20230725-0003/

Affected Product	**VMware**
Severity	**Medium**
Affected Vulnerability	Information Disclosure Vulnerability (CVE-2023-20891)
Description	VMware has released a security update addressing Information Disclosure vulnerability within VMware Tanzu Application Service for VMs and Isolation Segment. A malicious non-admin user who has access to the platform system audit logs can access hex encoded CF API admin credentials and can push new malicious versions of an application. VMware recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	VMware Tanzu Application Service for VMs 4.0.x VMware Tanzu Application Service for VMs 3.0.x VMware Tanzu Application Service for VMs 2.13.x VMware Tanzu Application Service for VMs 2.11.x Isolation Segment 4.0.x Isolation Segment 3.0.x Isolation Segment 2.13.x Isolation Segment 2.11.x
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.vmware.com/security/advisories/VMSA-2023-0016.html

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.