Advisory Alert

Alert Number: **AAA20230901** **Date:** **September 1, 2023**

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
HPE	**Critical**	Multiple vulnerabilities
VMware	**High**	SAML Token Signature Bypass vulnerability
Ivanti	**Medium**	Arbitrary code execution vulnerability

Description

Affected Product	**HPE**
Severity	**Critical**
Affected Vulnerability	Multiple vulnerabilities (CVE-2022-21449 ,CVE-2022-21476, CVE-2022-21426, CVE-2022-34169, CVE-2022-21248, CVE-2022-21277, CVE-2022-21282, CVE-2022-21283, CVE-2022-21291, CVE-2022-21293, CVE-2022-21294, CVE-2022-21296, CVE-2022-21299, CVE-2022-21305, CVE-2022-21340, CVE-2022-21341, CVE-2022-21349, CVE-2022-21360, CVE-2022-21365, CVE-2022-21366, CVE-2022-2625, CVE-2022-41946, CVE-2022-42889, CVE-2022-22950)
Description	HPE has released security updates addressing Multiple vulnerabilities that exist in HPE SANnav Management Software Multiple security vulnerabilities have been identified in the HPE B-Series SANnav Management Portal and HPE SANnav Global View, also known as HPE SANnav Management Software. The vulnerabilities could be locally and remotely exploited to disclose sensitive information, perform unauthorized access and modification of data, cause Denial of Service, perform remote code execution, buffer overflow, authentication bypass and privilege escalation. HPE recommends to apply the necessary security updates at earliest to avoid issues.
Affected Products	HPE SANnav Management Software - Prior to v2.3.0 and v2.2.2a
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbst04532en_us

Affected Product	**VMware**
Severity	**High**
Affected Vulnerability	SAML Token Signature Bypass vulnerability (CVE-2023-20900)
Description	VMware has released security updates addressing SAML Token Signature Bypass vulnerability that exist in the VMware tools. The vulnerability exists due to improper verification of SAML token signature. A remote attacker can bypass SAML token signature verification and perform man-in-the-middle (MITM) network positioning between vCenter server and the virtual machine. VMware recommends to apply the necessary security updates at earliest to avoid issues.
Affected Products	VMware Tools: 10.3.0 - 12.2.6 open-vm-tools: 10.3.0 - 12.2.5
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.vmware.com/security/advisories/VMSA-2023-0019.html

Affected Product	**Ivanti**
Severity	**Medium**
Affected Vulnerability	Arbitrary code execution vulnerability (CVE-2023-38036)
Description	Ivanti has released security updates addressing Arbitrary code execution vulnerability that exist in the Wavelink Avalanche Manager. An attacker can send a specially crafted message to the Wavelink Avalanche Manager, which could result in service disruption or arbitrary code execution Ivanti recommends to apply the necessary security updates at earliest to avoid issues.
Affected Products	Wavelink Avalanche versions 6.4.0 and older
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://forums.ivanti.com/s/article/Security-Advisory-Avalanche-CVE-2023-38036?language=en_US

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.