Advisory Alert

Alert Number: **AAA20231220** **Date:** **December 20, 2023**

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Ivanti	**Critical**	Multiple Vulnerabilities
HPE	**High**	Remote Authentication Bypass Vulnerability
Ivanti	**High, Medium**	Multiple Vulnerabilities

Description

Affected Product	**Ivanti**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-41727, CVE-2023-46216, CVE-2023-46217, CVE-2023-46220, CVE-2023-46221, CVE-2023-46222, CVE-2023-46223, CVE-2023-46224, CVE-2023-46225, CVE-2023-46257, CVE-2023-46258, CVE-2023-46259, CVE-2023-46261)
Description	Ivanti has released a security update addressing multiple critical vulnerabilities in Ivanti Avalanche products. An attacker may exploit these vulnerabilities to cause Buffer overflow and Remote Code Execution. Ivanti highly recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	Multiple Ivanti Avalanche Products
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://forums.ivanti.com/s/article/Avalanche-6-4-2-Security-Hardening-and-CVEs-addressed?language=en_US

Affected Product	**HPE**
Severity	**High**
Affected Vulnerability	Remote Authentication Bypass Vulnerability (CVE-2023-50272)
Description	HPE has released a security update addressing a potential remote authentication bypass vulnerability that exists in HPE Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 6 (iLO 6) products HPE recommends to apply the necessary security fixes at earliest to avoid issues.
Affected Products	HPE Integrated Lights-Out 5 (iLO 5) for HPE Gen10 Servers - v2.63 through versions prior to v3.00 HPE Integrated Lights-Out 6 (iLO 6) - v1.05 through versions prior to v1.55
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04584en_us

Affected Product	**Ivanti**
Severity	**High, Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-46260, CVE-2023-46262, CVE-2023-46266, CVE-2023-46263, CVE-2021-22962, CVE-2023-46264, CVE-2023-46265, CVE-2023-46803, CVE-2023-46804)
Description	Ivanti has released a security updates addressing multiple vulnerabilities in Ivanti Avalanche products. An attacker may exploit these vulnerabilities to cause Denial of Service, Server-Side Request Forgery, Remote Code Execution, Integer Underflow. Ivanti recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	Multiple Ivanti Avalanche products
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://forums.ivanti.com/s/article/Avalanche-6-4-2-Security-Hardening-and-CVEs-addressed?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.