Advisory Alert

Alert Number: AAA20250604 **Date:** June 4, 2025

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
HPE	**Critical**	Authentication Bypass Vulnerability
IBM	**Critical**	Multiple Vulnerabilities
SolarWinds	**High**	Local Privilege Escalation Vulnerability
Ubuntu	**High**	Multiple Linux kernel Vulnerabilities
HPE	**High**, Medium	Multiple Vulnerabilities
IBM	**High**, Medium, Low	Multiple Vulnerabilities

Description

Affected Product	**HPE**
Severity	**Critical**
Affected Vulnerability	Authentication Bypass Vulnerability (CVE-2025-37093)
Description	HPE has released security updates addressing an authentication bypass vulnerability that exists in HPE products. **CVE-2025-37093 -** An authentication bypass vulnerability exists in HPE StoreOnce Software. HPE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	HPE StoreOnce VSA - Prior to v4.3.11
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbst04847en_us&doc

Affected Product	**IBM**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-50379, CVE-2024-45337, CVE-2024-56337, CVE-2025-25022)
Description	IBM has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to cause Time-of-check Time-of-use (TOCTOU) Race Condition, Password in Configuration File and Authorization bypass. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM QRadar Suite Software - Versions 1.10.12.0 - 1.11.2.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.ibm.com/support/pages/node/7235402 • https://www.ibm.com/support/pages/node/7235432

Affected Product	**SolarWinds**
Severity	**High**
Affected Vulnerability	Local Privilege Escalation Vulnerability (CVE-2025-26396)
Description	SolarWinds has released security updates addressing multiple vulnerabilities that exist in their products. **CVE-2025-26396 -** The SolarWinds DameWare Mini Remote Control was determined to be affected by an incorrect permissions local privilege escalation vulnerability. This vulnerability requires local access and a valid low privilege account to be susceptible to this vulnerability. SolarWinds advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	SolarWinds Platform 12.3.1.20 and previous versions
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.solarwinds.com/trust-center/security-advisories/cve-2025-26396

Affected Product	**Ubuntu**
Severity	**High**
Affected Vulnerability	Multiple Linux kernel Vulnerabilities (CVE-2024-56608, CVE-2024-56551, CVE-2024-53168)
Description	Ubuntu has released security updates addressing multiple vulnerabilities that exist in their products. **CVE-2024-56608 -** An out-of-bound access can lead to local privilege escalation and arbitrary code execution. **CVE-2024-56551 -** A use-after-free can potentially end up with a local privilege escalation. **CVE-2024-53168 -** Use-after-frees can be utilized to gain privileges. Ubuntu advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Ubuntu 22.04
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://ubuntu.com/security/notices/USN-7550-1

Affected Product	**HPE**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-37089, CVE-2025-37090, CVE-2025-37091, CVE-2025-37092, CVE-2025-37094, CVE-2025-37095, CVE-2025-37096)
Description	HPE has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to cause Remote Code Execution, Server-Side Request Forgery and Directory Traversal Arbitrary File Deletion. HPE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	HPE StoreOnce VSA - Prior to v4.3.11
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbst04847en_us&doc

Affected Product	**IBM**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities
Description	IBM has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to cause Exposure of Sensitive Information to an Unauthorized Actor, Use of Uninitialized Variable, NULL Pointer Dereference, Out-of-bounds Write and Server-Side Request Forgery (SSRF). IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM QRadar Suite Software - Versions 1.10.12.0 - 1.11.2.0 IBM Db2 - Versions 11.1.0 - 11.1.4.7, 11.5.0 - 11.5.9, 12.1.0 - 12.1.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.ibm.com/support/pages/node/7235402 • https://www.ibm.com/support/pages/node/7235432 • https://www.ibm.com/support/pages/node/7235067

Disclaimer

The information provided are gathered from official service provider's websites and portals. FinCSIRT strongly recommends members to apply security fixes as per the given guidelines, following the organization's patch and change management procedures to protect systems from potential threats.