Advisory Alert

Alert Number: AAA20240426 **Date:** April 26, 2024

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
HPE	**Critical**	Multiple Vulnerabilities
IBM	**Medium**	Server-Side Request Forgery (SSRF) Vulnerability

Description

Affected Product	**HPE**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-29953, CVE-2022-25236, CVE-2019-6109, CVE-2023-2975 CVE-2023-0466, CVE-2023-0464)
Description	HPE has released security updates addressing multiple vulnerabilities that exist in HPE SAN Switches. HPE recommends to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	HPE B-series SN2600B SAN Extension Switch - Prior to v9.2.1, v9.2.0b and v9.1.1d HPE B-series SN3600B Fibre Channel Switch - Prior to v9.2.1, v9.2.0b and v9.1.1d HPE B-series SN6600B Fibre Channel Switch - Prior to v9.2.1, v9.2.0b and v9.1.1d HPE B-series SN6650B Fibre Channel Switch - Prior to v9.2.1, v9.2.0b and v9.1.1d HPE B-series SN6700B Fibre Channel Switch - Prior to v9.2.1, v9.2.0b and v9.1.1d HPE B-series SN6750B Fibre Channel Switch - Prior to v9.2.1, v9.2.0b and v9.1.1d HPE SN8600B 4-slot SAN Director Switch - Prior to v9.2.1, v9.2.0b and v9.1.1d HPE SN8600B 8-slot SAN Director Switch - Prior to v9.2.1, v9.2.0b and v9.1.1d HPE SN8700B 8-slot SAN Director Switch - Prior to v9.2.1, v9.2.0b and v9.1.1d HPE SN8700B 4-slot SAN Director Switch - Prior to v9.2.1, v9.2.0b and v9.1.1d Brocade 32Gb Fibre Channel SAN Switch for HPE Synergy - Prior to v9.2.1, v9.2.0b and v9.1.1d HPE B-series SN4700B SAN Extension Switch - Prior to v9.2.1 and v9.2.0b
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbst04635en_us&docLocale=en_US

Affected Product	**IBM**
Severity	**Medium**
Affected Vulnerability	Server-Side Request Forgery (SSRF) Vulnerability (CVE-2024-22329)
Description	IBM has released security update addressing a Server-Side Request Forgery (SSRF) Vulnerability that exists in IBM WebSphere Remote Server. An attacker could exploit this vulnerability by sending specially crafted request. IBM recommends to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM WebSphere Remote Server - Version(s) 9.1, 9.0, 8.5
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7149516

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.