Advisory Alert

Alert Number: **AAA20241029** **Date:** **October 29, 2024**

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Juniper	**Critical**	Multiple Vulnerabilities
FortiGuard	**Critical**	Arbitrary Code Execution Vulnerability
HPE	**High**	Unauthenticated Remote Code Execution Vulnerability

Description

Affected Product	**Juniper**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-35116,CVE-2023-34453,CVE-2023-34455,CVE-2023-34454,CVE-2023-43642,CVE-2023-2976,CVE-2023-33201,CVE-2023-46136,CVE-2023-43804,CVE-2023-37920,CVE-2022-25883,CVE-2023-45133,CVE-2023-31484,CVE-2023-1370,CVE-2021-4048,CVE-2021-23445,CVE-2021-31684,CVE-2023-38019,CVE-2023-38020,CVE-2023-38263,CVE-2023-46308,CVE-2023-32006,CVE-2023-32002,CVE-2023-32559,CVE-2022-38900,CVE-2023-45857,CVE-2022-25927,CVE-2023-44270,CVE-2023-26159,CVE-2020-19909,CVE-2023-38546,CVE-2023-38545,CVE-2023-5678,CVE-2023-46218,CVE-2023-46219,CVE-2023-4807,CVE-2023-0727,CVE-2023-6129,CVE-2023-5363,CVE-2022-21216,CVE-2023-46234,CVE-2024-28849,CVE-2024-29041,CVE-2024-29180,CVE-2024-4067,CVE-2024-4068,CVE-2024-21501,CVE-2024-27088,CVE-2024-27982,CVE-2024-27983,CVE-2021-23727,CVE-2024-39338,CVE-2019-13224,CVE-2019-16163,CVE-2019-19012,CVE-2022-24735,CVE-2022-24736,CVE-2022-24834,CVE-2023-28856,CVE-2023-45145)
Description	Juniper has released security updates addressing Multiple Vulnerabilities that exists in their products. Exploitation of these vulnerabilities may lead to denial of service, out of bounds reads, directory traversal, information disclosure, remote code execution. Juniper advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Juniper Networks Juniper Secure Analytics Applications: • Log Collector Application prior to version v1.8.4 • SOAR Plugin Application prior to version 5.3.1 • Deployment Intelligence Application prior to 3.0.13 • User Behavior Analytics Application add-on prior to 4.1.14 • Pulse Application add-on prior to 2.2.12 • Assistant Application add-on prior to 3.8.0 • Use Case Manager Application add-on prior to 3.9.0 • WinCollect Standalone Agent prior to 10.1.8 • M7 Appliances prior to 4.0.0 • Log Source Management App prior to 7.0.8
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://supportportal.juniper.net/s/article/On-Demand-JSA-Series-Multiple-vulnerabilities-resolved-in-JSA-Applications?language=en_US

Affected Product	**FortiGuard**
Severity	**Critical**
Affected Vulnerability	Arbitrary Code Execution Vulnerability (CVE-2024-47575)
Description	FortiGuard has released security updates addressing an Arbitrary Code Execution Vulnerability that exists in their products. This vulnerability is due to a missing authentication in FortiManager fgfmd daemon. FortiGuard advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	FortiManager 7.6.0 FortiManager 7.4.0 through 7.4.4 FortiManager 7.2.0 through 7.2.7 FortiManager 7.0.0 through 7.0.12 FortiManager 6.4.0 through 6.4.14 FortiManager 6.2.0 through 6.2.12 FortiManager Cloud 7.4.1 through 7.4.4 FortiManager Cloud 7.2.1 through 7.2.7 FortiManager Cloud 7.0.1 through 7.0.12 FortiManager Cloud 6.4 all versions
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.fortiguard.com/psirt/FG-IR-24-423

Affected Product	**HPE**
Severity	**High**
Affected Vulnerability	Unauthenticated Remote Code Execution Vulnerability (CVE-2024-6387)
Description	HPE has released security updates addressing an Unauthenticated Remote Code Execution vulnerability that exists in the OpenSSH third-party product that in turn affects HPE products. **CVE-2024-6387** - A security regression (CVE-2006-5051) was discovered in OpenSSH's server (sshd). There is a race condition which can lead sshd to handle some signals in an unsafe manner. An unauthenticated, remote attacker may be able to trigger it by failing to authenticate within a set time period. HPE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	HP-UX 11i Secure Shell Software prior to A.09.30.007
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbux04725en_us&docLocale=en_US

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.