TLP: WHITE

Advisory Alert

Alert Number: **AAA20230818** **Date:** **August 18, 2023**

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Juniper	**Critical**	Remote Code Execution
Fortinet	**Medium**	Buffer overflow vulnerability
CPanel	**Medium**	Multiple vulnerabilities

Description

Affected Product	**Juniper**
Severity	**Critical**
Affected Vulnerability	Remote Code Execution (CVE-2023-36844, CVE-2023-36845, CVE-2023-36846, CVE-2023-36847)
Description	Juniper has released security updates addressing Remote Code Execution that exist in their products. By chaining exploitation of these vulnerabilities, an unauthenticated, network-based attacker may be able to remotely execute code on the devices Juniper recommends to apply the necessary security updates at earliest to avoid issues.

Affected Products	Juniper Networks Junos OS on SRX Series
	All versions prior to 20.4R3-S8;
	21.2 versions prior to 21.2R3-S6;
	21.3 versions prior to 21.3R3-S5;
	21.4 versions prior to 21.4R3-S5;
	22.1 versions prior to 22.1R3-S3;
	22.2 versions prior to 22.2R3-S2;
	22.3 versions prior to 22.3R2-S2, 22.3R3;
	22.4 versions prior to 22.4R2-S1, 22.4R3;
	Juniper Networks Junos OS on EX Series:
	All versions prior to 20.4R3-S8;
	21.2 versions prior to 21.2R3-S6;
	21.3 versions prior to 21.3R3-S5;
	21.4 versions prior to 21.4R3-S4;
	22.1 versions prior to 22.1R3-S3;
	22.2 versions prior to 22.2R3-S1;
	22.3 versions prior to 22.3R2-S2, 22.3R3;
	22.4 versions prior to 22.4R2-S1, 22.4R3.

Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://supportportal.juniper.net/s/article/2023-08-Out-of-Cycle-Security-Bulletin-Junos-OS-SRX-Series-and-EX-Series-Multiple-vulnerabilities-in-J-Web-can-be-combined-to-allow-a-preAuth-Remote-Code-Execution?language=en_US

Affected Product	**Fortinet**
Severity	**Medium**
Affected Vulnerability	Buffer overflow vulnerability (CVE-2023-29182)
Description	Fortinet has released security updates addressing Buffer overflow vulnerability that exist in their FortiOS. The buffer overflow vulnerability in FortiOS may allow a privileged attacker to execute arbitrary code via specially crafted CLI commands, provided the attacker were able to evade FortiOS stack protections. Fortinet recommends to apply necessary security fixes at earliest to avoid issues.
Affected Products	FortiOS version 7.0.0 through 7.0.3 FortiOS 6.4 all versions FortiOS 6.2 all versions
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.fortiguard.com/psirt/FG-IR-23-149

Affected Product	**CPanel**
Severity	**Medium**
Affected Vulnerability	Multiple vulnerabilities (CVE-2023-32559, CVE-2023-32006, CVE-2023-32002)
Description	CPanel has released security updates addressing multiple vulnerabilities that exist in their cPanel EasyApache. The vulnerability allows a remote attacker to bypass implemented security restrictions as follow **CVE-2023-32559** - A remote attacker can bypass the policy mechanism by requiring internal modules and eventually take advantage of process.binding('spawn_sync') run arbitrary code, outside of the limits defined in a policy.json file. **CVE-2023-32006** –Due to improperly imposed security restrictions for module.constructor.createRequire() can bypass the policy mechanism and require modules outside of the policy.json definition for a given module. **CVE-2023-32002** - Due to improperly imposed security restrictions for the Module._load() method. A remote attacker can bypass the policy mechanism and include modules outside of the policy.json definition for a given module. CPanel recommends to apply necessary security fixes at earliest to avoid issues.
Affected Products	EasyApache 4 All versions of NodeJS through 16.20.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://news.cpanel.com/easyapache4-2023-08-16-maintenance-and-security-release/

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.