Advisory Alert

Alert Number: AAA20230714 **Date:** July 14, 2023

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Juniper	**Critical**	Multiple Vulnerabilities
Juniper	**High, Medium**	Multiple Vulnerabilities

Description

Affected Product	**Juniper**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-31629 , CVE-2022-31628, CVE-2022-31627, CVE-2022-31626, CVE-2022-31625, CVE-2021-21708, CVE-2021-21707, CVE-2021-21705, CVE-2021-21704, CVE-2021-21703, CVE-2021-21702, CVE-2020-7071)
Description	Juniper has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could exploited by attackers to bypass security restrictions, execute arbitrary code, denial of service, SSRF attacks and inject arbitrary XML code. Juniper recommends to apply the necessary security updates at earliest to avoid issues.
Affected Products	Junos OS when J-Web is enabled.
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://supportportal.juniper.net/s/article/2023-07-Security-Bulletin-Junos-OS-J-Web-Multiple-Vulnerabilities-in-PHP-software?language=en_US

Affected Product	**Juniper**
Severity	**High, Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2020-13817, CVE-2020-11868, CVE-2023-28985, CVE-2017-7653, CVE-2017-7654, CVE-2017-7655, CVE-2022-41974, CVE-2022-42898, CVE-2021-26401, CVE-2022-2964, CVE-2020-13946, CVE-2022-38023, CVE-2022-42703, CVE-2022-4378, CVE-2021-25220, CVE-2022-2795, CVE-2023-36831, CVE-2023-36835, CVE-2023-36834, CVE-2023-36833, CVE-2023-36840, CVE-2023-36850, CVE-2023-36848, CVE-2023-36836, CVE-2023-36838, CVE-2023-36849)
Description	Juniper has released security updates addressing multiple vulnerabilities that exist in their Junos OS. These vulnerabilities may result in a denial of service. Juniper recommends to apply necessary security fixes at earliest to avoid issues.
Affected Products	Multiple Products
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://supportportal.juniper.net/s/global-search/%40uri?language=-en_US#sort=relevancy&f:ctype=[Security%20Advisories]&f:slevel=[High,Medium]

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.