Advisory Alert

Alert Number: AAA20240112 **Date:** January 12, 2024

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Juniper	**Critical**	Multiple Vulnerabilities
ManageEngine	**High**	Remote Code execution Vulnerability
Juniper	**High**, **Medium**	Multiple Vulnerabilities

Description

Affected Product	**Juniper**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-0934, CVE-2023-22081, CVE-2023-3341, CVE-2023-2650, CVE-2023-3446, CVE-2023-3817, CVE-2020-12321, CVE-2023-22045, CVE-2023-22049, CVE-2023-32360, CVE-2022-41974, CVE-2023-38802, CVE-2023-20569, CVE-2023-20593, CVE-2022-42896, CVE-2023-1281, CVE-2023-1829, CVE-2023-2124, CVE-2023-2194, CVE-2023-2235, CVE-2023-38408, CVE-2023-2828, CVE-2023-21930, CVE-2023-21937, CVE-2023-21938, CVE-2023-21939, CVE-2023-21954, CVE-2023-21967, CVE-2023-21968, CVE-2023-24329, CVE-2023-32067, CVE-2021-26341, CVE-2021-33655, CVE-2021-33656, CVE-2022-1462, CVE-2022-1679, CVE-2022-1789, CVE-2022-20141, CVE-2022-2196, CVE-2022-25265, CVE-2022-2663, CVE-2022-3028, CVE-2022-30594, CVE-2022-3239, CVE-2022-3524, CVE-2022-3564, CVE-2022-3566, CVE-2022-3567, CVE-2022-3619, CVE-2022-3623, CVE-2022-3625, CVE-2022-3628, CVE-2022-3707, CVE-2022-39188, CVE-2022-39189, CVE-2022-41218, CVE-2022-4129, CVE-2022-41674, CVE-2022-42703, CVE-2022-42720, CVE-2022-42721, CVE-2022-42722, CVE-2022-43750, CVE-2022-47929, CVE-2023-0394, CVE-2023-0461, CVE-2023-1195, CVE-2023-1582, CVE-2023-23454, CVE-2022-4269, CVE-2022-4378, CVE-2023-0266, CVE-2023-0386, CVE-2023-23918, CVE-2023-23920, CVE-2023-0767, CVE-2023-0286, CVE-2022-2873, CVE-2022-41222, CVE-2022-43945, CVE-2022-37434, CVE-2022-38023, CVE-2021-25220, CVE-2022-2795, CVE-2022-4254, CVE-2023-21830, CVE-2023-21843, CVE-2023-22809, CVE-2022-2964, CVE-2022-4139, CVE-2016-2183, CVE-2019-17571, CVE-2020-9493, CVE-2022-23302, CVE-2022-23305, CVE-2022-23307, CVE-2023-26464, CVE-2021-44228, CVE-2021-44832, CVE-2020-0465, CVE-2020-0466, CVE-2021-0920, CVE-2021-26691, CVE-2021-34798, CVE-2021-3564, CVE-2021-3573, CVE-2021-3621, CVE-2021-3752, CVE-2021-39275, CVE-2021-4155, CVE-2021-44790, CVE-2022-0330, CVE-2022-22942, CVE-2024-21591)
Description	Juniper has released a security update addressing multiple vulnerabilities that exists in their products. If exploited these vulnerabilities could leads to Remote Code Execution, privilege escalation, heap overflow, NULL pointer dereference, flaw double-free memory corruption. Juniper highly recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	Juniper CTPView all versions Session Smart Router prior to SSR-6.2.3-r2 Security Director Insights all versions All versions of Junos OS on SRX Series and EX Series
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://supportportal.juniper.net/s/article/2024-01-Security-Bulletin-CTPView-Multiple-vulnerabilities-in-CTPView-CVE-yyyy-nnnn?language=en_US https://supportportal.juniper.net/s/article/2024-01-Security-Bulletin-Session-Smart-Router-Multiple-vulnerabilities-resolved?language=en_US https://supportportal.juniper.net/s/article/2024-01-Security-Bulletin-Security-Director-Insights-Multiple-vulnerabilities-in-SDI?language=en_US https://supportportal.juniper.net/s/article/2024-01-Security-Bulletin-Junos-OS-SRX-Series-and-EX-Series-Security-Vulnerability-in-J-web-allows-a-preAuth-Remote-Code-Execution-CVE-2024-21591?language=en_US

Affected Product	**ManageEngine**
Severity	**High**
Affected Vulnerability	Remote Code execution Vulnerability (CVE-2024-0252)
Description	ManageEngine has released a security update addressing a Remote Code execution Vulnerability that exists in ManageEngine ADSelfService Plus. By exploiting an authenticated user can execute remote codes on the machine where ADSelfService Plus is installed regardless of load balancer configurations. It is recommended by ManageEngine to apply necessary security fixes at earliest to avoid issues
.Affected Products	ManageEngine ADSelfService Plus Builds 6401 and older
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.manageengine.com/products/self-service-password/advisory/CVE-2024-0252.html

Affected Product	**Juniper**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-21595, CVE-2024-21616, CVE-2023-36842, CVE-2024-21604, CVE-2024-21599, CVE-2024-21607, CVE-2024-21585, CVE-2022-21699, CVE-2024-21606, CVE-2024-21603, CVE-2024-21613, CVE-2024-21594, CVE-2024-21612, CVE-2024-21614, CVE-2024-21602, CVE-2024-21601, CVE-2024-21587, CVE-2024-21589, CVE-2024-21597)
Description	Juniper has released security updates addressing multiple vulnerabilities that exists in their products. If exploited these vulnerabilities could lead to denial of service, arbitrary code execution, Heap-based Buffer Overflow, Sensitive information disclosure and access bypass. It is recommended by Juniper to apply necessary security fixes at earliest to avoid issues
.Affected Products	Multiple juniper products
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://supportportal.juniper.net/s/global-search/%40uri?language=en_US#sort=%40sfcec_community_publish_date_formula__c%20descending&f:ctype=[Security%20Advisories]

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.