



CVE-2020-1616

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2020-1616
State	PUBLIC
Assigner	sirt@juniper.net
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-04-08 20:15:00 UTC
Updated	2020-04-14 18:53:00 UTC
Description	Due to insufficient server-side login attempt limit enforcement, a vulnerability in the SSH login service of Juniper Networks J

Risk And Classification

Problem Types: CWE-307

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Juniper	Advanced Threat Protection	All	All	All	All
Application	Juniper	Advanced Threat Protection	All	All	All	All
Application	Juniper	Virtual Advanced Threat Protection	All	All	All	All
Application	Juniper	Virtual Advanced Threat Protection	All	All	All	All

References

Reference
2020-04 Security Bulletin: JATP Series: JATP Is susceptible to slow brute force attacks on the SSH service. (CVE-2020-1616) - Juniper Netwo
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report