# CVE Detail – CVE-2019-0039

If REST API is enabled, the Junos OS login credentials are vulnerable to brute force attacks. The high default connection limit of the REST API may allow an attacker to brute-force passwords using advanced scripting techniques. Additionally, administrators who do not enforce a strong password policy can increase the likelihood of success from brute force attacks. Affected releases are Juniper Networks Junos OS: 14.1X53 versions prior to 14.1X53-D49; 15.1 versions prior to 15.1F6-S12, 15.1R7-S3; 15.1X49 versions prior to 15.1X49-D160; 15.1X53 versions prior to 15.1X53-D236, 15.1X53-D495, 15.1X53-D591, 15.1X53-D69; 16.1 versions prior to 16.1R3-S10, 16.1R4-S12, 16.1R6-S6, 16.1R7-S3; 16.1X65 versions prior to 16.1X65-D49; 16.2 versions prior to 16.2R2-S7; 17.1 versions prior to 17.1R2-S10, 17.1R3; 17.2 versions prior to 17.2R1-S8, 17.2R3-S1; 17.3 versions prior to 17.3R3-S2; 17.4 versions prior to 17.4R1-S6, 17.4R2-S2; 18.1 versions prior to 18.1R2-S4, 18.1R3-S1; 18.2 versions prior to 18.2R1-S5; 18.2X75 versions prior to 18.2X75-D30; 18.3 versions prior to 18.3R1-S1.

## Threat-Mapped Scoring

Score: 3.25

Priority: P2 - Serious (High)

## EPSS

EPSS Score: N/A

Percentile: 0.51955

## CVSS Scoring

CVSS v3.1 Score: 8.1

Severity: HIGH

## Mapped CWE(s)

* CWE-307: Improper Restriction of Excessive Authentication Attempts

## CAPEC(s)

* CAPEC-16: Dictionary-based Password Attack
* CAPEC-49: Password Brute Forcing
* CAPEC-560: Use of Known Domain Credentials
* CAPEC-565: Password Spraying
* CAPEC-600: Credential Stuffing
* CAPEC-652: Use of Known Kerberos Credentials
* CAPEC-653: Use of Known Operating System Credentials

## ATT&CK Techniques

* T1110.001: Password Guessing
* T1558: Steal or Forge Kerberos Tickets
* T1110.003: Password Spraying
* T1078: Valid Accounts
* T1110.004: Credential Stuffing

## Used By (Actors/Tools)

* TrickBot (malware)
* Linux Rabbit (malware)
* Pony (malware)
* Bad Rabbit (malware)
* Emotet (malware)
* P.A.S. Webshell (malware)
* Lucifer (malware)
* China Chopper (malware)
* SeaDuke (malware)
* Duqu (malware)
* Xbash (malware)
* SpeakUp (malware)
* Kinsing (malware)
* Industroyer (malware)
* Dtrack (malware)
* HermeticWizard (malware)
* MailSniper (tool)
* CrackMapExec (tool)
* Indrik Spider (intrusion-set)
* Operation Wocao (campaign)
* Wizard Spider (intrusion-set)
* FIN7 (intrusion-set)
* Dragonfly (intrusion-set)
* OilRig (intrusion-set)
* Fox Kitten (intrusion-set)
* SolarWinds Compromise (campaign)
* Lazarus Group (intrusion-set)
* Play (intrusion-set)
* Sandworm Team (intrusion-set)
* Suckfly (intrusion-set)
* Ember Bear (intrusion-set)
* FIN6 (intrusion-set)
* Silence (intrusion-set)
* APT28 (intrusion-set)
* Cinnamon Tempest (intrusion-set)
* HEXANE (intrusion-set)
* Ke3chang (intrusion-set)
* Volt Typhoon (intrusion-set)
* Leafminer (intrusion-set)
* APT29 (intrusion-set)
* HAFNIUM (intrusion-set)
* APT39 (intrusion-set)
* POLONIUM (intrusion-set)
* Leviathan (intrusion-set)
* Akira (intrusion-set)
* LAPSUS$ (intrusion-set)
* Chimera (intrusion-set)
* menuPass (intrusion-set)
* 2015 Ukraine Electric Power Attack (campaign)
* APT41 (intrusion-set)
* INC Ransom (intrusion-set)
* GALLIUM (intrusion-set)
* FIN10 (intrusion-set)
* FIN8 (intrusion-set)
* FIN4 (intrusion-set)
* BlackByte (intrusion-set)
* Threat Group-3390 (intrusion-set)
* APT28 Nearest Neighbor Campaign (campaign)
* Night Dragon (campaign)
* Agrius (intrusion-set)
* Sea Turtle (intrusion-set)
* Leviathan Australian Intrusions (campaign)
* Axiom (intrusion-set)
* Operation MidnightEclipse (campaign)
* C0032 (campaign)
* HomeLand Justice (campaign)
* FIN5 (intrusion-set)
* APT33 (intrusion-set)
* Silent Librarian (intrusion-set)
* APT18 (intrusion-set)
* Carbanak (intrusion-set)
* Star Blizzard (intrusion-set)
* PittyTiger (intrusion-set)

## Affected Products

* cpe:2.3:o:juniper:junos:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:juniper:junos:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:juniper:junos:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:juniper:junos:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:juniper:junos:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:juniper:junos:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:juniper:junos:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:juniper:junos:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:juniper:junos:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:juniper:junos:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:juniper:junos:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:juniper:junos:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:juniper:junos:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:juniper:junos:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:juniper:junos:\*:\*:\*:\*:\*:\*:\*:\*