



CVE-2017-10601

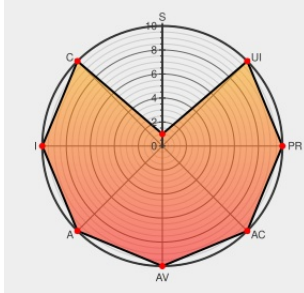
Published on: 07/14/2017 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:28 PM UTC

CVE-2017-10601

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#)

CVSS:30/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H



Certain versions of [Junos](#) from [Juniper](#) contain the following vulnerability:

A specific device configuration can result in a commit failure condition. When this occurs, a user is logged in without being prompted for a password while trying to login through console, ssh, ftp, telnet or su, etc., This issue relies upon a device configuration precondition to occur. Typically, device configurations are the result of a trusted

administrative change to the system's running configuration. The following error messages may be seen when this failure occurs: mgd: error: commit failed: (statements constraint check failed) Warning: Commit failed, activating partial configuration. Warning: Edit the router configuration to fix these errors. If the administrative changes are not made that result in such a failure, then this issue is not seen. No other Juniper Networks products or platforms are affected by this issue. Affected releases are Juniper Networks Junos OS 12.3 prior to 12.3R10, 12.3R11; 12.3X48 prior to 12.3X48-D20; 13.2 prior to 13.2R8; 13.3 prior to 13.3R7; 14.1 prior to 14.1R4-S12, 14.1R5, 14.1R6; 14.1X53 prior to 14.1X53-D30; 14.2 prior to 14.2R4; 15.1 prior to 15.1F2, 15.1F3, 15.1R2.

CVE-2017-10601 has been assigned by [J sirt@juniper.net](#) to track the vulnerability - currently rated as **CRITICAL** severity.

Vulnerability Patch/Work Around

Make sure authentication works as expected after a system configuration change. Use the SSH certificate based authentication. Use access lists or firewall filters to limit access to the device only from trusted administrative hosts, networks and users.

CVSS3 Score: **9.8 - CRITICAL**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: **10 - HIGH**

**Access
Vector**

NETWORK

**Access
Complexity**

LOW

Authentication

NONE

**Confidentiality
Impact**

COMPLETE

**Integrity
Impact**

COMPLETE

**Availability
Impact**

COMPLETE

CVE References

Description

Tags

Link

2017-07 Security Bulletin: Junos OS: Insufficient authentication for user login when a specific system configuration error occurs. (CVE-2017-10601) - Juniper Networks

Mitigation

Vendor Advisory

kb.juniper.net

text/html

 **CONFIRM**
kb.juniper.net/JSA10802

Juniper Junos Configuration Error Lets Remote Users Bypass Authentication and Access the Target System - SecurityTracker

Third Party Advisory

VDB Entry

www.securitytracker.com

text/html

 **SECTRAK**
1038902

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Juniper	Junos	12.3	All	All	All
Operating System	Juniper	Junos	12.3	r1	All	All
Operating System	Juniper	Junos	12.3	r11	All	All
Operating System	Juniper	Junos	12.3	r2	All	All
Operating System	Juniper	Junos	12.3	r3	All	All
Operating System	Juniper	Junos	12.3	r4	All	All
Operating System	Juniper	Junos	12.3	r5	All	All
Operating System	Juniper	Junos	12.3	r6	All	All
Operating System	Juniper	Junos	12.3	r7	All	All

Operating System	Juniper	Junos	12.3	r8	All	All
Operating System	Juniper	Junos	12.3	r9	All	All
Operating System	Juniper	Junos	12.3x48	d10	All	All
Operating System	Juniper	Junos	12.3x48	d15	All	All
Operating System	Juniper	Junos	13.2	All	All	All
Operating System	Juniper	Junos	13.2	r1	All	All
Operating System	Juniper	Junos	13.2	r2	All	All
Operating System	Juniper	Junos	13.2	r3	All	All
Operating System	Juniper	Junos	13.2	r4	All	All
Operating System	Juniper	Junos	13.2	r5	All	All
Operating System	Juniper	Junos	13.2	r6	All	All
Operating System	Juniper	Junos	13.2	r7	All	All
Operating System	Juniper	Junos	13.2	r7-s1	All	All
Operating System	Juniper	Junos	13.2	r7-s2	All	All
Operating System	Juniper	Junos	13.3	All	All	All
Operating System	Juniper	Junos	13.3	r2	All	All
Operating System	Juniper	Junos	13.3	r3	All	All
Operating System	Juniper	Junos	13.3	r4	All	All
Operating System	Juniper	Junos	13.3	r5	All	All
Operating System	Juniper	Junos	13.3	r6	All	All
Operating System	Juniper	Junos	14.1	All	All	All
Operating System	Juniper	Junos	14.1	r1	All	All
Operating System	Juniper	Junos	14.1	r2	All	All

Operating System	Juniper	Junos	14.1	r3	All	All
Operating System	Juniper	Junos	14.1	r4	All	All
Operating System	Juniper	Junos	14.1	r5	All	All
Operating System	Juniper	Junos	14.1	r6	All	All
Operating System	Juniper	Junos	14.1x53	All	All	All
Operating System	Juniper	Junos	14.1x53	d10	All	All
Operating System	Juniper	Junos	14.1x53	d15	All	All
Operating System	Juniper	Junos	14.1x53	d16	All	All
Operating System	Juniper	Junos	14.1x53	d25	All	All
Operating System	Juniper	Junos	14.1x53	d26	All	All
Operating System	Juniper	Junos	14.1x53	d27	All	All
Operating System	Juniper	Junos	14.2	All	All	All
Operating System	Juniper	Junos	14.2	r1	All	All
Operating System	Juniper	Junos	14.2	r2	All	All
Operating System	Juniper	Junos	14.2	r3	All	All
Operating System	Juniper	Junos	14.2	r4	All	All
Operating System	Juniper	Junos	15.1	All	All	All
Operating System	Juniper	Junos	15.1	f1	All	All
Operating System	Juniper	Junos	15.1	f2	All	All
Operating System	Juniper	Junos	15.1	f3	All	All
Operating System	Juniper	Junos	15.1	r2	All	All
Operating System	Juniper	Junos	12.3	All	All	All
Operating System	Juniper	Junos	12.3	r1	All	All

System						
Operating System	Juniper	Junos	12.3	r11	All	All
Operating System	Juniper	Junos	12.3	r2	All	All
Operating System	Juniper	Junos	12.3	r3	All	All
Operating System	Juniper	Junos	12.3	r4	All	All
Operating System	Juniper	Junos	12.3	r5	All	All
Operating System	Juniper	Junos	12.3	r6	All	All
Operating System	Juniper	Junos	12.3	r7	All	All
Operating System	Juniper	Junos	12.3	r8	All	All
Operating System	Juniper	Junos	12.3	r9	All	All
Operating System	Juniper	Junos	12.3x48	d10	All	All
Operating System	Juniper	Junos	12.3x48	d15	All	All
Operating System	Juniper	Junos	13.2	All	All	All
Operating System	Juniper	Junos	13.2	r1	All	All
Operating System	Juniper	Junos	13.2	r2	All	All
Operating System	Juniper	Junos	13.2	r3	All	All
Operating System	Juniper	Junos	13.2	r4	All	All
Operating System	Juniper	Junos	13.2	r5	All	All
Operating System	Juniper	Junos	13.2	r6	All	All
Operating System	Juniper	Junos	13.2	r7	All	All
Operating System	Juniper	Junos	13.2	r7-s1	All	All
Operating System	Juniper	Junos	13.2	r7-s2	All	All
Operating System	Juniper	Junos	13.3	All	All	All
Operating System	Juniper	Junos	13.3	r2	All	All

System						
Operating System	Juniper	Junos	13.3	r3	All	All
Operating System	Juniper	Junos	13.3	r4	All	All
Operating System	Juniper	Junos	13.3	r5	All	All
Operating System	Juniper	Junos	13.3	r6	All	All
Operating System	Juniper	Junos	14.1	All	All	All
Operating System	Juniper	Junos	14.1	r1	All	All
Operating System	Juniper	Junos	14.1	r2	All	All
Operating System	Juniper	Junos	14.1	r3	All	All
Operating System	Juniper	Junos	14.1	r4	All	All
Operating System	Juniper	Junos	14.1	r5	All	All
Operating System	Juniper	Junos	14.1	r6	All	All
Operating System	Juniper	Junos	14.1x53	All	All	All
Operating System	Juniper	Junos	14.1x53	d10	All	All
Operating System	Juniper	Junos	14.1x53	d15	All	All
Operating System	Juniper	Junos	14.1x53	d16	All	All
Operating System	Juniper	Junos	14.1x53	d25	All	All
Operating System	Juniper	Junos	14.1x53	d26	All	All
Operating System	Juniper	Junos	14.1x53	d27	All	All
Operating System	Juniper	Junos	14.2	All	All	All
Operating System	Juniper	Junos	14.2	r1	All	All
Operating System	Juniper	Junos	14.2	r2	All	All
Operating System	Juniper	Junos	14.2	r3	All	All
Operating System	Juniper	Junos	14.2	r4	All	All

System						
Operating System	Juniper	Junos	15.1	All	All	All
Operating System	Juniper	Junos	15.1	f1	All	All
Operating System	Juniper	Junos	15.1	f2	All	All
Operating System	Juniper	Junos	15.1	f3	All	All
Operating System	Juniper	Junos	15.1	r2	All	All
cpe:2.3:o:juniper:junos:12.3:*:*:*:*:*:						
cpe:2.3:o:juniper:junos:12.3:r1:*:*:*:*:*:						
cpe:2.3:o:juniper:junos:12.3:r11:*:*:*:*:*:						
cpe:2.3:o:juniper:junos:12.3:r2:*:*:*:*:*:						
cpe:2.3:o:juniper:junos:12.3:r3:*:*:*:*:*:						
cpe:2.3:o:juniper:junos:12.3:r4:*:*:*:*:*:						
cpe:2.3:o:juniper:junos:12.3:r5:*:*:*:*:*:						
cpe:2.3:o:juniper:junos:12.3:r6:*:*:*:*:*:						
cpe:2.3:o:juniper:junos:12.3:r7:*:*:*:*:*:						
cpe:2.3:o:juniper:junos:12.3:r8:*:*:*:*:*:						
cpe:2.3:o:juniper:junos:12.3:r9:*:*:*:*:*:						
cpe:2.3:o:juniper:junos:12.3x48:d10:*:*:*:*:*:						
cpe:2.3:o:juniper:junos:12.3x48:d15:*:*:*:*:*:						
cpe:2.3:o:juniper:junos:13.2:*:*:*:*:*:						
cpe:2.3:o:juniper:junos:13.2:r1:*:*:*:*:*:						
cpe:2.3:o:juniper:junos:13.2:r2:*:*:*:*:*:						
cpe:2.3:o:juniper:junos:13.2:r3:*:*:*:*:*:						
cpe:2.3:o:juniper:junos:13.2:r4:*:*:*:*:*:						
cpe:2.3:o:juniper:junos:13.2:r5:*:*:*:*:*:						
cpe:2.3:o:juniper:junos:13.2:r6:*:*:*:*:*:						
cpe:2.3:o:juniper:junos:13.2:r7:*:*:*:*:*:						
cpe:2.3:o:juniper:junos:13.2:r7-s1:*:*:*:*:*:						

cpe:2.3:o:juniper:junos:13.2:r7-s2:~::~~::~~::~~::~~::
cpe:2.3:o:juniper:junos:13.3:~::~~::~~::~~::~~::
cpe:2.3:o:juniper:junos:13.3:r2:~::~~::~~::~~::~~::
cpe:2.3:o:juniper:junos:13.3:r3:~::~~::~~::~~::~~::
cpe:2.3:o:juniper:junos:13.3:r4:~::~~::~~::~~::~~::
cpe:2.3:o:juniper:junos:13.3:r5:~::~~::~~::~~::~~::
cpe:2.3:o:juniper:junos:13.3:r6:~::~~::~~::~~::~~::
cpe:2.3:o:juniper:junos:14.1:~::~~::~~::~~::~~::
cpe:2.3:o:juniper:junos:14.1:r1:~::~~::~~::~~::~~::
cpe:2.3:o:juniper:junos:14.1:r2:~::~~::~~::~~::~~::
cpe:2.3:o:juniper:junos:14.1:r3:~::~~::~~::~~::~~::
cpe:2.3:o:juniper:junos:14.1:r4:~::~~::~~::~~::~~::
cpe:2.3:o:juniper:junos:14.1:r5:~::~~::~~::~~::~~::
cpe:2.3:o:juniper:junos:14.1:r6:~::~~::~~::~~::~~::
cpe:2.3:o:juniper:junos:14.1x53:~::~~::~~::~~::~~::
cpe:2.3:o:juniper:junos:14.1x53:d10:~::~~::~~::~~::~~::
cpe:2.3:o:juniper:junos:14.1x53:d15:~::~~::~~::~~::~~::
cpe:2.3:o:juniper:junos:14.1x53:d16:~::~~::~~::~~::~~::
cpe:2.3:o:juniper:junos:14.1x53:d25:~::~~::~~::~~::~~::
cpe:2.3:o:juniper:junos:14.1x53:d26:~::~~::~~::~~::~~::
cpe:2.3:o:juniper:junos:14.1x53:d27:~::~~::~~::~~::~~::
cpe:2.3:o:juniper:junos:14.2:~::~~::~~::~~::~~::
cpe:2.3:o:juniper:junos:14.2:r1:~::~~::~~::~~::~~::
cpe:2.3:o:juniper:junos:14.2:r2:~::~~::~~::~~::~~::
cpe:2.3:o:juniper:junos:14.2:r3:~::~~::~~::~~::~~::
cpe:2.3:o:juniper:junos:14.2:r4:~::~~::~~::~~::~~::
cpe:2.3:o:juniper:junos:15.1:~::~~::~~::~~::~~::
cpe:2.3:o:juniper:junos:15.1:f1:~::~~::~~::~~::~~::

cpe:2.3:o:juniper:junos:15.1:f2:~::~~::~~::~~::~::
cpe:2.3:o:juniper:junos:15.1:f3:~::~~::~~::~~::~::
cpe:2.3:o:juniper:junos:15.1:r2:~::~~::~~::~~::~::
cpe:2.3:o:juniper:junos:12.3:~::~~::~~::~~::~::
cpe:2.3:o:juniper:junos:12.3:r1:~::~~::~~::~~::~::
cpe:2.3:o:juniper:junos:12.3:r11:~::~~::~~::~~::~::
cpe:2.3:o:juniper:junos:12.3:r2:~::~~::~~::~~::~::
cpe:2.3:o:juniper:junos:12.3:r3:~::~~::~~::~~::~::
cpe:2.3:o:juniper:junos:12.3:r4:~::~~::~~::~~::~::
cpe:2.3:o:juniper:junos:12.3:r5:~::~~::~~::~~::~::
cpe:2.3:o:juniper:junos:12.3:r6:~::~~::~~::~~::~::
cpe:2.3:o:juniper:junos:12.3:r7:~::~~::~~::~~::~::
cpe:2.3:o:juniper:junos:12.3:r8:~::~~::~~::~~::~::
cpe:2.3:o:juniper:junos:12.3:r9:~::~~::~~::~~::~::
cpe:2.3:o:juniper:junos:12.3x48:d10:~::~~::~~::~~::~::
cpe:2.3:o:juniper:junos:12.3x48:d15:~::~~::~~::~~::~::
cpe:2.3:o:juniper:junos:13.2:~::~~::~~::~~::~::
cpe:2.3:o:juniper:junos:13.2:r1:~::~~::~~::~~::~::
cpe:2.3:o:juniper:junos:13.2:r2:~::~~::~~::~~::~::
cpe:2.3:o:juniper:junos:13.2:r3:~::~~::~~::~~::~::
cpe:2.3:o:juniper:junos:13.2:r4:~::~~::~~::~~::~::
cpe:2.3:o:juniper:junos:13.2:r5:~::~~::~~::~~::~::
cpe:2.3:o:juniper:junos:13.2:r6:~::~~::~~::~~::~::
cpe:2.3:o:juniper:junos:13.2:r7:~::~~::~~::~~::~::
cpe:2.3:o:juniper:junos:13.2:r7-s1:~::~~::~~::~~::~::
cpe:2.3:o:juniper:junos:13.2:r7-s2:~::~~::~~::~~::~::
cpe:2.3:o:juniper:junos:13.3:~::~~::~~::~~::~::
cpe:2.3:o:juniper:junos:13.3:r2:~::~~::~~::~~::~::
cpe:2.3:o:iuniper:iunos:13.3:r3:~::~~::~~::~~::~::

Appendix A

```
cpe:2.3:o:juniper:junos:13.3:r4:*:*:*:*:*:
```

```
cpe:2.3:o:juniper:junos:13.3:r5:*:*:*:*:*:
```

```
cpe:2.3:o:juniper:junos:13.3:r6:*:*:*:*:*:
```

```
cpe:2.3:o:juniper:junos:14.1:*:*:*:*:*:*:
```

```
cpe:2.3:o:juniper:junos:14.1:r1:*:*:*:*:*:
```

```
cpe:2.3:o:juniper:junos:14.1:r2:*:*:*:*:*:
```

```
cpe:2.3:o:juniper:junos:14.1:r3:*:*:*:*:*:
```

```
cpe:2.3:o:juniper:junos:14.1:r4:*:*:*:*:*:
```

```
cpe:2.3:o:juniper:junos:14.1:r5:*:*:*:*:*:
```

```
cpe:2.3:o:juniper:junos:14.1:r6:*:*:*:*:*:
```

```
cpe:2.3:o:juniper:junos:14.1x53:*:*:*:*:*:
```

```
cpe:2.3:o:juniper:junos:14.1x53:d10:*:*:*:*:*:
```

```
cpe:2.3:o:juniper:junos:14.1x53:d15:*:*:*:*:*:
```

```
cpe:2.3:o:juniper:junos:14.1x53:d16:*:*:*:*:*:
```

```
cpe:2.3:o:juniper:junos:14.1x53:d25:*:*:*:*:*:
```

```
cpe:2.3:o:juniper:junos:14.1x53:d26:*:*:*:*:*:
```

```
cpe:2.3:o:juniper:junos:14.1x53:d27:*:*:*:*:*:
```

```
cpe:2.3:o:juniper:junos:14.2:*:*:*:*:*:*:
```

```
cpe:2.3:o:juniper:junos:14.2:r1:*:*:*:*:*:
```

```
cpe:2.3:o:juniper:junos:14.2:r2:*:*:*:*:*:
```

```
cpe:2.3:o:juniper:junos:14.2:r3:*:*:*:*:*:
```

```
cpe:2.3:o:juniper:junos:14.2:r4:*:*:*:*:*:
```

```
cpe:2.3:o:juniper:junos:15.1:*:*:*:*:*:*:
```

```
cpe:2.3:o:juniper:junos:15.1:f1:*:*:*:*:*:
```

```
cpe:2.3:o:juniper:junos:15.1:f2:*:*:*:*:*:
```

```
cpe:2.3:o:juniper:junos:15.1:f3:*:*:*:*:*:
```

```
cpe:2.3:o:juniper:junos:15.1:r2:*:*:*:*:*:
```

© [CVE.report](#) 2023  |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to 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](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)