



CVE-2018-0057

Published on: 10/10/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:49 PM UTC

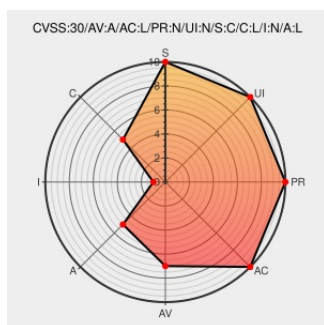
CVE-2018-0057 - advisory for JSA10892

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



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

On MX Series and M120/M320 platforms configured in a Broadband Edge (BBE) environment, subscribers logging in with DHCP Option 50 to request a specific IP address will be assigned the requested IP address, even if there is a static MAC to IP address binding in the access profile. In the problem scenario, with a hardware-address and

IP address configured under address-assignment pool, if a subscriber logging in with DHCP Option 50, the subscriber will not be assigned an available address from the matched pool, but will still get the requested IP address. A malicious DHCP subscriber may be able to utilize this vulnerability to create duplicate IP address assignments, leading to a denial of service for valid subscribers or unauthorized information disclosure via IP address assignment spoofing. Affected releases are Juniper Networks Junos OS: 15.1 versions prior to 15.1R7-S2, 15.1R8; 16.1 versions prior to 16.1R4-S12, 16.1R7-S2, 16.1R8; 16.2 versions prior to 16.2R2-S7, 16.2R3; 17.1 versions prior to 17.1R2-S9, 17.1R3; 17.2 versions prior to 17.2R1-S7, 17.2R2-S6, 17.2R3; 17.3 versions prior to 17.3R2-S4, 17.3R3; 17.4 versions prior to 17.4R2; 18.1 versions prior to 18.1R2-S3, 18.1R3.

CVE-2018-0057 has been assigned by [JJ](#) sirt@juniper.net to track the vulnerability - currently rated as **CRITICAL** severity.

Juniper SIRT is not aware of any malicious exploitation of this vulnerability.

Vulnerability Patch/Work Around

There are no viable workarounds for this issue

CVSS3 Score: **9.6 - CRITICAL**

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

impact		impact	impact
CHANGED	HIGH	NONE	HIGH
CVSS2 Score: 5.5 - MEDIUM			
Access Vector	Access Complexity	Authentication	
NETWORK	LOW	SINGLE	
Confidentiality Impact	Integrity Impact	Availability Impact	
PARTIAL	NONE	PARTIAL	

CVE References		
Description	Tags	Link
2018-10 Security Bulletin: Junos OS: authd allows assignment of IP address requested by DHCP subscriber logging in with Option 50 (Requested IP Address) (CVE-2018-0057) - Juniper Networks	Vendor Advisory kb.juniper.net text/html	 CONFIRM kb.juniper.net/JSA10892
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	15.1	All	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	f4	All	All
Operating System	Juniper	Junos	15.1	f5	All	All
Operating System	Juniper	Junos	15.1	f6	All	All
Operating System	Juniper	Junos	15.1	r1	All	All
Operating System	Juniper	Junos	15.1	r2	All	All
Operating System	Juniper	Junos	15.1	r3	All	All
Operating System	Juniper	Junos	15.1	r4	All	All

Operating System	Juniper	Junos	15.1	r5	All	All
Operating System	Juniper	Junos	15.1	r6	All	All
Operating System	Juniper	Junos	16.1	All	All	All
Operating System	Juniper	Junos	16.1	r1	All	All
Operating System	Juniper	Junos	16.1	r2	All	All
Operating System	Juniper	Junos	16.1	r3	All	All
Operating System	Juniper	Junos	16.2	All	All	All
Operating System	Juniper	Junos	16.2	r1	All	All
Operating System	Juniper	Junos	17.1	All	All	All
Operating System	Juniper	Junos	17.1	r1	All	All
Operating System	Juniper	Junos	17.2	All	All	All
Operating System	Juniper	Junos	17.3	All	All	All
Operating System	Juniper	Junos	17.3	r1	All	All
Operating System	Juniper	Junos	17.4	All	All	All
Operating System	Juniper	Junos	17.4	r1	All	All
Operating System	Juniper	Junos	18.1	All	All	All
Operating System	Juniper	Junos	18.1	r1	All	All
Operating System	Juniper	Junos	15.1	All	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	f4	All	All
Operating System	Juniper	Junos	15.1	f5	All	All
Operating System	Juniper	Junos	15.1	f6	All	All

Operating System	Juniper	Junos	15.1	r1	All	All
Operating System	Juniper	Junos	15.1	r2	All	All
Operating System	Juniper	Junos	15.1	r3	All	All
Operating System	Juniper	Junos	15.1	r4	All	All
Operating System	Juniper	Junos	15.1	r5	All	All
Operating System	Juniper	Junos	15.1	r6	All	All
Operating System	Juniper	Junos	16.1	All	All	All
Operating System	Juniper	Junos	16.1	r1	All	All
Operating System	Juniper	Junos	16.1	r2	All	All
Operating System	Juniper	Junos	16.1	r3	All	All
Operating System	Juniper	Junos	16.2	All	All	All
Operating System	Juniper	Junos	16.2	r1	All	All
Operating System	Juniper	Junos	17.1	All	All	All
Operating System	Juniper	Junos	17.1	r1	All	All
Operating System	Juniper	Junos	17.2	All	All	All
Operating System	Juniper	Junos	17.3	All	All	All
Operating System	Juniper	Junos	17.3	r1	All	All
Operating System	Juniper	Junos	17.4	All	All	All
Operating System	Juniper	Junos	17.4	r1	All	All
Operating System	Juniper	Junos	18.1	All	All	All
Operating System	Juniper	Junos	18.1	r1	All	All
cpe:2.3:o:juniper:junos:15.1:****:*:*:						
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:f4:~::~~::~~::~~::~::
cpe:2.3:o:juniper:junos:15.1:f5:~::~~::~~::~~::~::
cpe:2.3:o:juniper:junos:15.1:f6:~::~~::~~::~~::~::
cpe:2.3:o:juniper:junos:15.1:r1:~::~~::~~::~~::~::
cpe:2.3:o:juniper:junos:15.1:r2:~::~~::~~::~~::~::
cpe:2.3:o:juniper:junos:15.1:r3:~::~~::~~::~~::~::
cpe:2.3:o:juniper:junos:15.1:r4:~::~~::~~::~~::~::
cpe:2.3:o:juniper:junos:15.1:r5:~::~~::~~::~~::~::
cpe:2.3:o:juniper:junos:15.1:r6:~::~~::~~::~~::~::
cpe:2.3:o:juniper:junos:16.1:~::~~::~~::~~::~::
cpe:2.3:o:juniper:junos:16.1:r1:~::~~::~~::~~::~::
cpe:2.3:o:juniper:junos:16.1:r2:~::~~::~~::~~::~::
cpe:2.3:o:juniper:junos:16.1:r3:~::~~::~~::~~::~::
cpe:2.3:o:juniper:junos:16.2:~::~~::~~::~~::~::
cpe:2.3:o:juniper:junos:16.2:r1:~::~~::~~::~~::~::
cpe:2.3:o:juniper:junos:17.1:~::~~::~~::~~::~::
cpe:2.3:o:juniper:junos:17.1:r1:~::~~::~~::~~::~::
cpe:2.3:o:juniper:junos:17.2:~::~~::~~::~~::~::
cpe:2.3:o:juniper:junos:17.3:~::~~::~~::~~::~::
cpe:2.3:o:juniper:junos:17.3:r1:~::~~::~~::~~::~::
cpe:2.3:o:juniper:junos:17.4:~::~~::~~::~~::~::
cpe:2.3:o:juniper:junos:17.4:r1:~::~~::~~::~~::~::
cpe:2.3:o:juniper:junos:18.1:~::~~::~~::~~::~::
cpe:2.3:o:juniper:junos:18.1:r1:~::~~::~~::~~::~::
cpe:2.3:o:juniper:junos:15.1:~::~~::~~::~~::~::
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:f4:~::~~::~~::~~::~::

cpe:2.3:o:juniper:junos:15.1:f5:~::~~::
cpe:2.3:o:juniper:junos:15.1:f6:~::~~::
cpe:2.3:o:juniper:junos:15.1:r1:~::~~::
cpe:2.3:o:juniper:junos:15.1:r2:~::~~::
cpe:2.3:o:juniper:junos:15.1:r3:~::~~::
cpe:2.3:o:juniper:junos:15.1:r4:~::~~::
cpe:2.3:o:juniper:junos:15.1:r5:~::~~::
cpe:2.3:o:juniper:junos:15.1:r6:~::~~::
cpe:2.3:o:juniper:junos:16.1:~::~~::
cpe:2.3:o:juniper:junos:16.1:r1:~::~~::
cpe:2.3:o:juniper:junos:16.1:r2:~::~~::
cpe:2.3:o:juniper:junos:16.1:r3:~::~~::
cpe:2.3:o:juniper:junos:16.2:~::~~::
cpe:2.3:o:juniper:junos:16.2:r1:~::~~::
cpe:2.3:o:juniper:junos:17.1:~::~~::
cpe:2.3:o:juniper:junos:17.1:r1:~::~~::
cpe:2.3:o:juniper:junos:17.2:~::~~::
cpe:2.3:o:juniper:junos:17.3:~::~~::
cpe:2.3:o:juniper:junos:17.3:r1:~::~~::
cpe:2.3:o:juniper:junos:17.4:~::~~::
cpe:2.3:o:juniper:junos:17.4:r1:~::~~::
cpe:2.3:o:juniper:junos:18.1:~::~~::
cpe:2.3:o:juniper:junos:18.1:r1:~::~~::

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)

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](#)