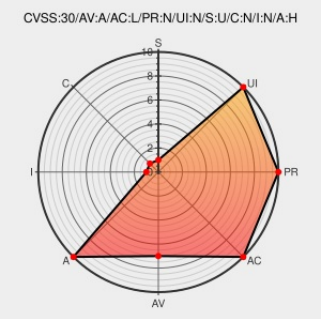
CVE-2018-0006

Published on: 01/10/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:48 PM UTC

CVE-2018-0006 - advisory for JSA10834

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Junos from Juniper contain the following vulnerability:

A high rate of VLAN authentication attempts sent from an adjacent host on the local broadcast domain can trigger high memory utilization by the BBE subscriber management daemon (bbe-smgd), and lead to a denial of service condition. The issue was caused by attempting to process an unbounded number of pending VLAN authentication requests, leading to excessive memory allocation. This issue only affects devices configured for DHCPv4/v6 over AE auto-sensed VLANs, utilized in Broadband Edge (BBE) deployments. Other configurations are unaffected by this issue. Affected releases are Juniper Networks Junos OS: 15.1 versions prior to 15.1R6-S2, 15.1R7; 16.1 versions prior to 16.1R5-S1, 16.1R6; 16.2 versions prior to 16.2R2-S2, 16.2R3; 17.1 versions prior to 17.1R2-S5, 17.1R3; 17.2 versions prior to 17.2R2.

CVE-2018-0006 has been assigned by sirt@juniper.net to track the vulnerability - currently rated as MEDIUM severity.

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

Affected Vendor/Software: **Juniper Networks** - **Junos OS** version **15.1R6-S2, 15.1R7**

Affected Vendor/Software: **Juniper Networks** - **Junos OS** version **16.1R5-S1, 16.1R6**

Affected Vendor/Software: **Juniper Networks** - **Junos OS** version **16.2R2-S2, 16.2R3**

Affected Vendor/Software: **Juniper Networks** - **Junos OS** version **17.1R2-S5, 17.1R3**

Affected Vendor/Software: **Juniper Networks** - **Junos OS** version **17.2R2**

Vulnerability Patch/Work Around

Since this issue is specific to auto-sense or dynamic VLANs, utilizing a static VLAN model will mitigate this issue.

CVSS3 Score: 5.3 - MEDIUM

Attack	Attack	Privileges	User

Vector	Complexity	Required	Interaction
ADJACENT_NETWORK	HIGH	NONE	NONE

Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	NONE	NONE	HIGH

CVSS2 Score: 2.9 - LOW

Access Vector	Access Complexity	Authentication
ADJACENT_NETWORK	MEDIUM	NONE

Confidentiality Impact	Integrity Impact	Availability Impact
NONE	NONE	PARTIAL

CVE References

Description	Tags	Link
2018-01 Security Bulletin: Junos: bbe-smgd process denial of service while processing VLAN authentication requests/rejects (CVE-2018-0006) - Juniper Networks	Mitigation, Patch, Vendor Advisory, kb.juniper.net, text/html	CONFIRM kb.juniper.net/JSA10834
Juniper Junos bbe-smgd VLAN Authentication Processing Flaw Lets Remote Users Consume Excessive Memory Resources - SecurityTracker	Third Party Advisory, VDB Entry, www.securitytracker.com, text/html	SECTRACK 1040184

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	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	Juniper	Junos	15.1	r5	All	All

System						
Operating System	Juniper	Junos	15.1	r7	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	16.1	r4	All	All
Operating System	Juniper	Junos	16.1	r6	All	All
Operating System	Juniper	Junos	16.2	r1	All	All
Operating System	Juniper	Junos	16.2	r3	All	All
Operating System	Juniper	Junos	17.1	r1	All	All
Operating System	Juniper	Junos	17.1	r3	All	All
Operating System	Juniper	Junos	17.2	r1	All	All
Operating System	Juniper	Junos	15.1	All	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	r7	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	Juniper	Junos	16.1	r3	All	All

System						
Operating System	Juniper	Junos	16.1	r4	All	All
Operating System	Juniper	Junos	16.1	r6	All	All
Operating System	Juniper	Junos	16.2	r1	All	All
Operating System	Juniper	Junos	16.2	r3	All	All
Operating System	Juniper	Junos	17.1	r1	All	All
Operating System	Juniper	Junos	17.1	r3	All	All
Operating System	Juniper	Junos	17.2	r1	All	All

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

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:r7:*:*:*:*:*:*:

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:16.1:r4:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:16.1:r6:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:16.2:r1:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:16.2:r3:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:17.1:r1:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:17.1:r3:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:17.2:r1:*:*:*:*:*:*:

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

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:r7:*:*:*:*:*:*:

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:16.1:r4:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:16.1:r6:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:16.2:r1:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:16.2:r3:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:17.1:r1:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:17.1:r3:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:17.2:r1:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→