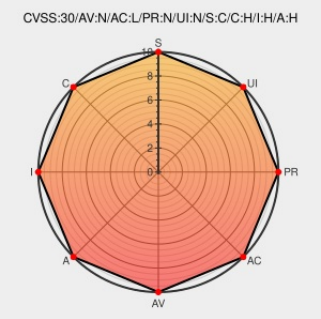
CVE-2017-2343

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

Last Modified on: 03/23/2021 11:26:53 PM UTC

CVE-2017-2343

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



Certain versions of Junos from Juniper contain the following vulnerability:

The Integrated User Firewall (UserFW) feature was introduced in Junos OS version 12.1X47-D10 on the Juniper SRX Series devices to provide simple integration of user profiles on top of the existing firewall polices. As part of an internal security review of the UserFW services authentication API, hardcoded credentials were identified and removed which can impact both the SRX Series device, and potentially LDAP and Active Directory integrated points. An attacker may be able to completely compromise SRX Series devices, as well as Active Directory servers and services. When Active Directory is compromised, it may allow access to user credentials, workstations, servers performing other functions such as email, database, etc. Inter-Forest Active Directory deployments may also be at risk as the attacker may gain full administrative control over one or more Active Directories depending on the credentials supplied by the administrator of the AD domains and SRX devices performing integrated authentication of users, groups and devices. To identify if your device is potentially vulnerable to exploitation, check to see if the service is operating; from CLI review the following output: root@SRX-Firewall# run show services user-identification active-directory-access domain-controller status extensive A result of "Status: Connected" will indicate that the service is active on the device. To evaluate if user authentication is occurring through the device: root@SRX-Firewall# run show services user-identification active-directory-access active-directory-authentication-table all Next review the results to see if valid users and groups are returned. e.g. Domain: juniperlab.com Total entries: 3 Source IP Username groups state 172.16.26.1 administrator Valid 192.168.26.2 engg01 engineers Valid 192.168.26.3 guest01 guests Valid Domain: NULL Total entries: 8 Source IP Username groups state 192.168.26.4 Invalid 192.168.26.5 Invalid This will also indicate that Valid users and groups are authenticating through the device. Affected releases are Juniper Networks Junos OS 12.3X48 from 12.3X48-D30 and prior to 12.3X48-D35 on SRX series; 15.1X49 from 15.1X49-D40 and prior to 15.1X49-D50 on SRX series. Devices on any version of Junos OS 12.1X46, or 12.1X47 are unaffected by this issue.

CVE-2017-2343 has been assigned by sirt@juniper.net to track the vulnerability - currently rated as CRITICAL severity.

Affected Vendor/Software: **Juniper Networks** - **Junos OS** version **12.3X48 from 12.3X48-D30 and prior to 12.3X48-D35**

Affected Vendor/Software: **Juniper Networks** - **Junos OS** version **15.1X49 from 15.1X49-D40 and prior to 15.1X49-D50**

Vulnerability Patch/Work Around

There is no workaround to completely mitigate the risk of this issue. Customers may reduce the risk of exploitation of this issue by disabling the UserFW service on devices running the service until such time that a fix can be taken.

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	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
2017-07 Security Bulletin: SRX Series: Hardcoded credentials in Integrated UserFW feature. (CVE-2017-2343) - Juniper Networks	Vendor Advisory kb.juniper.net text/html	CONFIRM kb.juniper.net/JSA10791
Juniper Junos Default Credentials in SRX Series Integrated User Firewall Lets Remote Users Access the Target System - SecurityTracker	Third Party Advisory VDB Entry www.securitytracker.com text/html	SECTRACK 1038904

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	12.3x48	d10	All	All

Operating System	Juniper	Junos	12.3x48	d15	All	All
Operating System	Juniper	Junos	12.3x48	d20	All	All
Operating System	Juniper	Junos	12.3x48	d25	All	All
Operating System	Juniper	Junos	12.3x48	d30	All	All
Operating System	Juniper	Junos	12.3x48	d35	All	All
Operating System	Juniper	Junos	15.1x49	d40	All	All
Operating System	Juniper	Junos	15.1x49	d45	All	All
Operating System	Juniper	Junos	12.3x48	d10	All	All
Operating System	Juniper	Junos	12.3x48	d15	All	All
Operating System	Juniper	Junos	12.3x48	d20	All	All
Operating System	Juniper	Junos	12.3x48	d25	All	All
Operating System	Juniper	Junos	12.3x48	d30	All	All
Operating System	Juniper	Junos	12.3x48	d35	All	All
Operating System	Juniper	Junos	15.1x49	d40	All	All
Operating System	Juniper	Junos	15.1x49	d45	All	All
Hardware	Juniper	Srx100	-	All	All	All
Hardware	Juniper	Srx100	-	All	All	All
Hardware	Juniper	Srx110	-	All	All	All
Hardware	Juniper	Srx110	-	All	All	All
Hardware	Juniper	Srx1400	-	All	All	All
Hardware	Juniper	Srx1400	-	All	All	All
Hardware	Juniper	Srx210	-	All	All	All
Hardware	Juniper	Srx210	-	All	All	All
Hardware	Juniper	Srx220	-	All	All	All
Hardware	Juniper	Srx220	-	All	All	All

Hardware	Juniper	Srx240	-	All	All	All
Hardware	Juniper	Srx240	-	All	All	All
Hardware	Juniper	Srx3400	-	All	All	All
Hardware	Juniper	Srx3400	-	All	All	All
Hardware	Juniper	Srx3600	-	All	All	All
Hardware	Juniper	Srx3600	-	All	All	All
Hardware	Juniper	Srx5400	-	All	All	All
Hardware	Juniper	Srx5400	-	All	All	All
Hardware	Juniper	Srx550	-	All	All	All
Hardware	Juniper	Srx550	-	All	All	All
Hardware	Juniper	Srx5600	-	All	All	All
Hardware	Juniper	Srx5600	-	All	All	All
Hardware	Juniper	Srx5800	-	All	All	All
Hardware	Juniper	Srx5800	-	All	All	All
Hardware	Juniper	Srx650	-	All	All	All
Hardware	Juniper	Srx650	-	All	All	All

cpe:2.3:o:juniper:junos:12.3x48:d10:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:12.3x48:d15:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:12.3x48:d20:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:12.3x48:d25:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:12.3x48:d30:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:12.3x48:d35:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:15.1x49:d40:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:15.1x49:d45:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:12.3x48:d10:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:12.3x48:d15:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:12.3x48:d20:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:12.3x48:d25:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:12.3x48:d30:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:12.3x48:d35:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:15.1x49:d40:*:*:*:*:*:*:*

cpe:2.3:o:juniper:junos:15.1x49:d45:*:*:*:*:*:*:*

cpe:2.3:h:juniper:srx100:-:*:*:*:*:*:*:*:*

cpe:2.3:h:juniper:srx100:-:*:*:*:*:*:*:*:*

cpe:2.3:h:juniper:srx110:-:*:*:*:*:*:*:*:*

cpe:2.3:h:juniper:srx110:-:*:*:*:*:*:*:*:*

cpe:2.3:h:juniper:srx1400:-:*:*:*:*:*:*:*:*

cpe:2.3:h:juniper:srx1400:-:*:*:*:*:*:*:*:*

cpe:2.3:h:juniper:srx210:-:*:*:*:*:*:*:*:*

cpe:2.3:h:juniper:srx210:-:*:*:*:*:*:*:*:*

cpe:2.3:h:juniper:srx220:-:*:*:*:*:*:*:*:*

cpe:2.3:h:juniper:srx220:-:*:*:*:*:*:*:*:*

cpe:2.3:h:juniper:srx240:-:*:*:*:*:*:*:*:*

cpe:2.3:h:juniper:srx240:-:*:*:*:*:*:*:*:*

cpe:2.3:h:juniper:srx3400:-:*:*:*:*:*:*:*:*

cpe:2.3:h:juniper:srx3400:-:*:*:*:*:*:*:*:*

cpe:2.3:h:juniper:srx3600:-:*:*:*:*:*:*:*:*

cpe:2.3:h:juniper:srx3600:-:*:*:*:*:*:*:*:*

cpe:2.3:h:juniper:srx5400:-:*:*:*:*:*:*:*:*

cpe:2.3:h:juniper:srx5400:-:*:*:*:*:*:*:*:*

cpe:2.3:h:juniper:srx550:-:*:*:*:*:*:*:*:*

cpe:2.3:h:juniper:srx550:-:*:*:*:*:*:*:*:*

cpe:2.3:h:juniper:srx5600:-:*:*:*:*:*:*:*:*

cpe:2.3:h:juniper:srx5600:-:*:*:*:*:*:*:*:*

cpe:2.3:h:juniper:srx5800:-:*:*:*:*:*:*:*:*

cpe:2.3:h:juniper:srx5800:-:*:*:*:*:*:*:*:*

cpe:2.3:h:juniper:srx650:-:*:*:*:*:*:*:*:*

cpe:2.3:h:juniper:srx650:-:*:*:*:*:*:*:*:*

← Previous ID

Next ID→

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