



CVE-2017-14695

Published on: 10/24/2017 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:45 PM UTC

CVE-2017-14695

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

Certain versions of [Salt](#) from [Saltstack](#) contain the following vulnerability:

Directory traversal vulnerability in minion id validation in SaltStack Salt before 2016.3.8, 2016.11.x before 2016.11.8, and 2017.7.x before 2017.7.2 allows remote minions with incorrect credentials to authenticate to a master via a crafted minion ID. NOTE: this vulnerability exists because of an incomplete fix for CVE-2017-12791.

CVE-2017-14695 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **CRITICAL** severity.

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: **7.5 - HIGH**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
Salt 2016.3.8 Release Notes	Issue Tracking Release Notes Vendor Advisory	docs.saltstack.com/en/latest/topics/releases/2016.3.8.html

	docs.saltstack.com text/html	
Salt 2016.11.8 Release Notes	Issue Tracking Release Notes Vendor Advisory docs.saltstack.com text/html	 CONFIRM docs.saltstack.com/en/latest/topics/releases/2016.11.8.html
openSUSE-SU-2017:2822-1: moderate: Security update for salt	Issue Tracking Release Notes Third Party Advisory lists.opensuse.org text/html	 SUSE openSUSE-SU-2017:2822
Salt 2017.7.2 Release Notes	Issue Tracking Release Notes Vendor Advisory docs.saltstack.com text/html	 CONFIRM docs.saltstack.com/en/latest/topics/releases/2017.7.2.html
openSUSE-SU-2017:2824-1: moderate: Security update for salt	Issue Tracking Release Notes Third Party Advisory lists.opensuse.org text/html	 SUSE openSUSE-SU-2017:2824
1500748 – (CVE-2017-14695) CVE-2017-14695 salt: Directory traversal in minion id validation	Issue Tracking Release Notes Third Party Advisory bugzilla.redhat.com text/html	 CONFIRM bugzilla.redhat.com/show_bug.cgi?id=1500748
Don't allow path separators in minion ID · saltstack/salt@80d9030 · GitHub	Issue Tracking Patch Third Party Advisory github.com text/html	 CONFIRM github.com/saltstack/salt/commit/80d90307b07b3703428ecbb7c8bb468e28a9ae6d

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
Application	Saltstack	Salt	2016.11	All	All	All
Application	Saltstack	Salt	2016.11.0	All	All	All
Application	Saltstack	Salt	2016.11.1	All	All	All
Application	Saltstack	Salt	2016.11.1	rc1	All	All
Application	Saltstack	Salt	2016.11.1	rc2	All	All
Application	Saltstack	Salt	2016.11.2	All	All	All
Application	Saltstack	Salt	2016.11.3	All	All	All
Application	Saltstack	Salt	2016.11.4	All	All	All

Application	Saltstack	Salt	2016.11.4	All	All	All
Application	Saltstack	Salt	2016.11.5	All	All	All
Application	Saltstack	Salt	2016.11.6	All	All	All
Application	Saltstack	Salt	2016.11.7	All	All	All
Application	Saltstack	Salt	2017.7.0	All	All	All
Application	Saltstack	Salt	2017.7.0	rc1	All	All
Application	Saltstack	Salt	2017.7.1	All	All	All
Application	Saltstack	Salt	2016.11	All	All	All
Application	Saltstack	Salt	2016.11.0	All	All	All
Application	Saltstack	Salt	2016.11.1	All	All	All
Application	Saltstack	Salt	2016.11.1	rc1	All	All
Application	Saltstack	Salt	2016.11.1	rc2	All	All
Application	Saltstack	Salt	2016.11.2	All	All	All
Application	Saltstack	Salt	2016.11.3	All	All	All
Application	Saltstack	Salt	2016.11.4	All	All	All
Application	Saltstack	Salt	2016.11.5	All	All	All
Application	Saltstack	Salt	2016.11.6	All	All	All
Application	Saltstack	Salt	2016.11.7	All	All	All
Application	Saltstack	Salt	2017.7.0	All	All	All
Application	Saltstack	Salt	2017.7.0	rc1	All	All
Application	Saltstack	Salt	2017.7.1	All	All	All
Application	Saltstack	Salt	All	All	All	All
cpe:2.3:a:saltstack:salt:2016.11:*****:*						
cpe:2.3:a:saltstack:salt:2016.11.0:*****:*						
cpe:2.3:a:saltstack:salt:2016.11.1:*****:*						
cpe:2.3:a:saltstack:salt:2016.11.1:rc1:*****:*						
cpe:2.3:a:saltstack:salt:2016.11.1:rc2:*****:*						
cpe:2.3:a:saltstack:salt:2016.11.2:*****:*						
cpe:2.3:a:saltstack:salt:2016.11.3:*****:*						
cpe:2.3:a:saltstack:salt:2016.11.4:*****:*						
cpe:2.3:a:saltstack:salt:2016.11.5:*****:*						
cpe:2.3:a:saltstack:salt:2016.11.6:*****:*						
cpe:2.3:a:saltstack:salt:2016.11.7:*****:*						

cpe:2.3:a:saltstack:salt:2017.7.0:*****:
cpe:2.3:a:saltstack:salt:2017.7.0:rc1:*****:
cpe:2.3:a:saltstack:salt:2017.7.1:*****:
cpe:2.3:a:saltstack:salt:2016.11:*****:
cpe:2.3:a:saltstack:salt:2016.11.0:*****:
cpe:2.3:a:saltstack:salt:2016.11.1:*****:
cpe:2.3:a:saltstack:salt:2016.11.1:rc1:*****:
cpe:2.3:a:saltstack:salt:2016.11.1:rc2:*****:
cpe:2.3:a:saltstack:salt:2016.11.2:*****:
cpe:2.3:a:saltstack:salt:2016.11.3:*****:
cpe:2.3:a:saltstack:salt:2016.11.4:*****:
cpe:2.3:a:saltstack:salt:2016.11.5:*****:
cpe:2.3:a:saltstack:salt:2016.11.6:*****:
cpe:2.3:a:saltstack:salt:2016.11.7:*****:
cpe:2.3:a:saltstack:salt:2017.7.0:*****:
cpe:2.3:a:saltstack:salt:2017.7.0:rc1:*****:
cpe:2.3:a:saltstack:salt:2017.7.1:*****:
cpe:2.3:a:saltstack:salt:*****:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)

© [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](#)