



# CVE-2020-11651

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2020-11651
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2020-04-30 17:15:00 UTC
<b>Updated</b>	2022-07-12 17:42:00 UTC
<b>Description</b>	An issue was discovered in SaltStack Salt before 2019.2.4 and 3000 before 3000.2. The salt-master process ClearFuncs cl

## Risk And Classification

**EPSS:** 0.944210000 probability, percentile 0.999810000 (date 2026-04-01)

**CISA KEV:** Listed on 2021-11-03; due 2022-05-03; ransomware use Unknown

**Problem Types:** NVD-CWE-Other

## CISA Known Exploited Vulnerability

<b>Vendor</b>	SaltStack
<b>Product</b>	Salt
<b>Name</b>	SaltStack Salt Authentication Bypass Vulnerability
<b>Required Action</b>	Apply updates per vendor instructions.
<b>Notes</b>	<a href="https://nvd.nist.gov/vuln/detail/CVE-2020-11651">https://nvd.nist.gov/vuln/detail/CVE-2020-11651</a>

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	16.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	18.04	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	10.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	8.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	9.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	10.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	9.0	All	All	All
Operating System	<a href="#">Opensuse</a>	<a href="#">Leap</a>	15.1	All	All	All

Operating System	<a href="#">Opensuse</a>	<a href="#">Leap</a>	15.1	All	All	All
Application	<a href="#">Saltstack</a>	<a href="#">Salt</a>	All	All	All	All
Application	<a href="#">Saltstack</a>	<a href="#">Salt</a>	All	All	All	All
Application	<a href="#">Vmware</a>	<a href="#">Application Remote Collector</a>	7.5.0	All	All	All
Application	<a href="#">Vmware</a>	<a href="#">Application Remote Collector</a>	8.0.0	All	All	All

## References

Reference	Source	Link	Tags
[security-announce] openSUSE-SU-2020:0564-1: critical: Security update f	SUSE	<a href="https://lists.opensuse.org">lists.opensuse.org</a>	Mailing List
Saltstack 3000.1 Remote Code Execution ~ Packet Storm	MISC	<a href="https://packetstormsecurity.com">packetstormsecurity.com</a>	Exploit, Thi
VMSA-2020-0009.1	CONFIRM	<a href="https://www.vmware.com">www.vmware.com</a>	
[SECURITY] [DLA 2223-1] salt security update	MLIST	<a href="https://lists.debian.org">lists.debian.org</a>	
USN-4459-1: Salt vulnerabilities   Ubuntu security notices   Ubuntu	UBUNTU	<a href="https://usn.ubuntu.com">usn.ubuntu.com</a>	
Salt 2019.2.4 Release Notes	MISC	<a href="https://docs.saltstack.com">docs.saltstack.com</a>	Vendor Adv
[security-announce] openSUSE-SU-2020:1074-1: moderate: Security update f	SUSE	<a href="https://lists.opensuse.org">lists.opensuse.org</a>	
SaltStack Salt Master/Minion Unauthenticated Remote Code Execution ~ Packet Storm	MISC	<a href="https://packetstormsecurity.com">packetstormsecurity.com</a>	
salt/3000.2.rst at v3000.2_docs · saltstack/salt · GitHub	MISC	<a href="https://github.com">github.com</a>	Third Party
SaltStack FrameWork Vulnerabilities Affecting Cisco Products	CISCO	<a href="https://tools.cisco.com">tools.cisco.com</a>	
Debian -- Security Information -- DSA-4676-1 salt	DEBIAN	<a href="https://www.debian.org">www.debian.org</a>	Third Party
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	canonical, i
CISA Known Exploited Vulnerabilities catalog	CISA	<a href="https://www.cisa.gov">www.cisa.gov</a>	kev

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

[374575](#) VMware vRealize Operations Application Remote Collector (ARC) Multiple Vulnerabilities (VMSA-2020-0009)

[501244](#) Alpine Linux Security Update for salt

[505396](#) Alpine Linux Security Update for salt

[750688](#) SUSE Enterprise Linux Security Update for salt (SUSE-SU-2021:2105-1)

[750705](#) OpenSUSE Security Update for salt (openSUSE-SU-2021:0899-1)

[750760](#) OpenSUSE Security Update for salt (openSUSE-SU-2021:2106-1)

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](#)**