

CVE-2020-11651

SaltStack Salt Authentication Bypass Vulnerability

Exigent

CISA KEV since Nov 3, 2021

Actively exploited

Public exploit module (Metasploit)

An issue was discovered in SaltStack Salt before 2019.2.4 and 3000 before 3000.2. The salt-master process ClearFuncs class does not properly validate method calls. This allows a remote user to access some methods without authentication. These methods can be used to retrieve user tokens from the salt master and/or run arbitrary commands on salt minions.

EVRS 86/100 Immediate priority	CVSS V3.1 9.8 Critical · NVD	EPSS 0.966 99.89th percentile · FIRST	CISA DEADLINE May 3, 2022 KEV since 2021 · listed over a year
--	--	---	---

Signals behind the score

☒ counted in the score ☐ not counted

evidence for 6 of 8 signals

☒ CISA KEV	Listed in the catalog	☐ Vendor exploitation	Confirmed exploitation in the wild
☐ Ransomware	No known ransomware campaign association	☐ KEV recency	On the CISA KEV catalog for over two years
☒ EPSS	0.966 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 9.8	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Out-of-band / urgent Patch or fixed version identified

CISA required action: Apply updates per vendor instructions.

Basis: CISA KEV required action

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
salt	< 2019.2.4 ≥ 3000 < 3000.2	no fixed version listed	NVD
application remote collector	7.5.0 8.0.0	no fixed version listed	NVD
leap	15.1	no fixed version listed	NVD
debian linux	8.0 9.0 10.0	no fixed version listed	NVD
ubuntu linux	16.04 18.04	no fixed version listed	NVD

Sources

Vendor guidance github.com/advisories/GHSA-pjhf-vpx3-33r3

Additional guidance docs.saltstack.com/en/latest/topics/releases/2019.2.4.html

NVD nvd.nist.gov/vuln/detail/CVE-2020-11651

CISA KEV cisa.gov/known-exploited-vulnerabilities-catalog

ENISA EUVD euvd.enisa.europa.eu/vulnerability/EUVD-2020-0171

Current data evulnable.com/vulnerability-management/cve/CVE-2020-11651

Snapshot at generation time. EPSS can move quickly. A public exploit module is not evidence of active exploitation.