

CVE-2020-16846

SaltStack Salt Shell Injection Vulnerability

Exigent

CISA KEV since Nov 3, 2021

Actively exploited

Public exploit module (Metasploit)

An issue was discovered in SaltStack Salt through 3002. Sending crafted web requests to the Salt API, with the SSH client enabled, can result in shell injection.

EVRS 87 / 100 Immediate priority	CVSS V3.1 9.8 Critical · NVD	EPSS 0.996 99.95th 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	0.996 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 · GHSA-qr38-h96j-2j3w lists 1 more affected package

PACKAGE	AFFECTED	FIXED IN	SOURCE
salt	< 2015.8.13	2015.8.13	GitHub
salt	≥ 2016.3.0, < 2016.3.8	2016.3.8	GitHub
salt	≥ 2016.11.0, < 2016.11.10	2016.11.10	GitHub
salt	≥ 2017.5.0, < 2017.7.8	2017.7.8	GitHub
salt	≥ 2018.2.0, < 2018.3.5	2018.3.5	GitHub
salt	≥ 2019.2.0, < 2019.2.6	2019.2.6	GitHub
salt	≥ 3000.0, < 3000.4	3000.4	GitHub
salt	≥ 3001, < 3001.2	3001.2	GitHub
debian linux	9.0 10.0	no fixed version listed	NVD
fedora	31	no fixed version listed	NVD
leap	15.1	no fixed version listed	NVD

Sources

Vendor guidance github.com/advisories/GHSA-qr38-h96j-2j3w

NVD nvd.nist.gov/vuln/detail/CVE-2020-16846

ENISA EUVD euvd.enisa.europa.eu/vulnerability/EUVD-2020-0173

Additional guidance saltstack.com/blog/on-november-3-2020-saltstack-publicly-disclosed-three-new-cves/cisa.gov/known-exploited-vulnerabilities-catalog

CISA KEV

Current data evulnable.com/vulnerability-management/cve/CVE-2020-16846

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