



CVE-2013-2228

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2013-2228
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-12-03 14:15:00 UTC
Updated	2019-12-13 15:33:00 UTC
Description	SaltStack RSA Key Generation allows remote users to decrypt communications

Risk And Classification

Problem Types: CWE-307

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Saltstack	Saltstack	All	All	All	All

References

Reference	Source
Bug 864236 – VUL-0: CVE-2013-2228: salt: RSA exponent set to 1	MISC
oss-security - CVE-2013-2228 : Salt Stack RSA exponent of 1 (there can be only one! da-na-naaah! na-na-na-naahh-nah-nahhh!)	MISC
IBM X-Force Exchange	MISC
475438 – (CVE-2013-2228) app-admin/salt: Multiple Vulnerabilities (CVE-2013-2228)	MISC
SaltStack RSA Key Generation Weakness Lets Remote Users Decrypt Communications in Certain Cases - SecurityTracker	MISC
CVE-2013-2228	MISC
SaltStack Salt Multiple Security Bypass and Command Injection Vulnerabilities	MISC
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](#) 2026 |

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](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)