Dear Community,

A critical vulnerability has been discovered in Salt master versions 3000.1 and earlier.

The vulnerability has been rated as critical with a Common Vulnerability Scoring System (CVSS) score of 10.0. Once SaltStack became aware of the vulnerability, we quickly took actions to remediate the vulnerability.

We are preparing to make a CVE release available on Wednesday, April 29th.  The CVE release will be 3000.2 and 2019.2.4.  The releases will only be containing the patches available to resolve and remediate the identified vulnerabilities.

We recommend you review this article to ensure you are actively following SaltStack's best practices for securing your Salt Environment: [Hardening Salt](). Specifically please ensure Salt masters are not exposed to the internet, and only authorized systems can connect to them.  These steps and best practices would ensure you are safeguarded.

To avoid unintended exposure or exploitation, further details will be shared closer to the release date.  Given the critical nature of the vulnerability we are advising all our users to quickly apply the CVE release as soon as the packages are available.

Please reach out, if you have any questions or comments.  You can reach us at security@saltstack.com

Thank you.
Your Salt Open Core team.