Mirantis Technical Bulletin 2020-002

June 01, 2020

SaltStack authentication bypass and directory traversal vulnerabilities (CVE-2020-11651, CVE-2020-11652)

ISSUE

Two critical vulnerabilities have been disclosed in SaltStack versions prior to 2019.2.4. The vulnerabilities are exploitable only if the Salt Master node is exposed to the Internet. The vulnerabilities may result in arbitrary directory access to unauthenticated users, retrieval of user tokens from the Salt Master node and/or execution of arbitrary commands on the Salt Minion nodes.

For more information, refer to CVE-2020-11651 and CVE-2020-11652.

AFFECTS

Any MCP version up to and including the 2019.2.9 maintenance update.

SECURITY IMPACT

High

RESOLUTION

The resolution is under development by the Mirantis product team and will be available as part of the 2019.2.10 maintenance update and announced separately.

In the meantime, Mirantis strongly encourages that you apply the SaltStack community recommendations for hardening the Salt Master nodes and follow MCP Reference Architecture recommendations for networking security to ensure that your cloud is not affected by the vulnerabilities.

