Security Disclosure Notice
October 1, 2019

Customer security is a top priority at Jamf. When an incident occurs, our teams are committed to protecting customers and sharing information as soon as we are able.

We recently became aware of a critical security vulnerability affecting multiple versions of Jamf Pro. On September 28, we upgraded all Standard Cloud customers and alerted all other customers to the issue and offered a path to mitigation. Now that all customers have had three days to upgrade, we are able to share additional information about the vulnerability.

The information below will add detail to what we've already released. If you have any additional questions, please reach out to success@jamf.com for more assistance.

Issue Summary

Jamf Pro is vulnerable to deserialization of untrusted data when parsing JSON in several APIs.

Issue Severity

Jamf uses the Common Vulnerability Scoring System (CVSS) to scope the severity of security issues.

This issue registers a CVSS version 3.1 score of: 10.0 (critical)

General information about the CVSS is available here: https://www.first.org/cvss/

Specific information about a CVSS score of 10.0 is available here: https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:H/A:H

Affected Versions

The following versions of Jamf Pro are affected by this issue:

Jamf Pro versions 9.4 to 9.101.4
Jamf Pro versions 10.0.0 to 10.15.0

Issue Description

A request containing specially crafted JSON that is sent to certain endpoints in Jamf Pro could result in the deletion of files on the server and/or Denial of Service (DoS). In affected versions of Jamf Pro prior to 10.14.0, these requests could also result in remote code execution (RCE).

Please note:

- This issue only impacts the Jamf Pro server and does not impact managed clients or client management functions.
- This issue only impacts files on the Jamf Pro server that are accessible to the user that is running the Jamf Pro process.

CWE Category

Deserialization of untrusted data: https://cwe.mitre.org/data/definitions/502.html

Mitigation

JSON parsers in Jamf Pro have been updated to include whitelisting and error handling so that only known classes and valid JSON are accepted for deserialization. Also, Jamf Cloud standard instances have been updated to Jamf Pro 10.15.1.

Next Steps

We strongly recommend all customers immediately upgrade to Jamf Pro 10.15.1.

- Standard Cloud: All Standard Cloud customers were upgraded to version 10.15.1 on September 28, 2019 as part of a rolling mass cloud upgrade. No additional action is needed.
- Premium Cloud & Custom Cloud: Contact success@jamf.com to schedule an upgrade to 10.15.1 as soon as possible.
- On-Premise: An installer for version 10.15.1 is available on the My Assets page on your administrator’s Jamf Nation account.

We recognize that some customers may not be able to immediately upgrade to version 10.15.1 due to a change in Java support. If you require support for Java 8, we are making a special build - Jamf Pro 10.13.1 - available as a path to mitigation. If you would like to upgrade to 10.13.1, please contact success@jamf.com.

As always, please contact success@jamf.com if you have any questions or concerns.