Jamf Pro - Detect and remediate Meltdown and Spectre vulnerabilities

Jamf Pro - Detect and remediate Meltdown and Spectre vulnerabilities

Meltdown and Spectre are the name for two security vulnerabilities made public in early 2018. This article will explain how to detect vulnerability of managed Macs with Jamf Pro and how to patch vulnerable components.

Vulnerable software versions

- All macOS versions older than 10.13.2. For systems running 10.13.2, confirm that Apple's supplemental update has been installed. For 10.12 Sierra and 10.11 El Capitan, Apple has released Security Update 2018-001, which patches Meltdown but not Spectre.
- All Safari versions older than 11.0.2. The Safari patch for High Sierra can be found in the supplemental update above. The patch for Sierra and El Capitan can be found here: https://support.apple.com/en-us/HT208403
- Firefox versions older than 57.0.4 in the primary release channel ("mainline"), and older than 52.6.0 in the Extended Support Release channel ("ESR").
- Google Chrome versions older than 64.0.

Detection in Casper

In the JSS, we've added an extension attribute called "Spectre/Meltdown Vulnerability". You can add this to your inventory display by following the instructions at Casper - Extension Attributes.

For macOS 10.13 High Sierra, it will show either "Patched" or "Vulnerable". For 10.11 and 10.12, it will show "Vulnerable" or "Meltdown-Patched" and "Spectre-Vulnerable", since Security Update 2018-001 only patches Meltdown. For Safari, Firefox, and Chrome, it will also show whether they are "Patched" or Vulnerable".

Recommendations

- All Macs should be upgraded to macOS High Sierra 10.13.3 or higher. Macs running OS X Yosemite (10.10) or older are especially vulnerable and should be a high priority to upgrade. See Casper - Upgrading Macs to latest operating system for instructions on upgrading to macOS High Sierra.
- Any Macs running OS X El Capitan (10.11) or macOS Sierra (10.12) that cannot be upgraded to High Sierra (10.13) should install all the latest patches from Apple, including the Safari patch and Security Update 2018-001. These OSes do not currently have patches for Spectre (only Meltdown), so again, it's recommended to upgrade to macOS High Sierra if possible. See Casper - Apple Software Updates for instructions on deploying Apple Software Updates with Casper, or follow the remediation instructions below.
- Any Macs running Firefox should be updated to at least 57.0.4 or ESR 52.6.0.
- Any Macs running Google Chrome should be updated to at least 64.0.

Remediation with Casper

The EPM team has set up two custom triggers to install relevant Meltdown/Spectre patches, **epm-spectre** and **epm-spectre-force**. You can call these from Terminal by entering e.g. **sudo jamf policy -event epm-spectre**, or call them via a Casper policy (see below).

The **epm-spectre** trigger is designed to be safe to run at any time without disrupting the user. It will skip OS updates that require a system reboot, and will only update Firefox and Chrome if they are not currently in use. This is ideal to run in the background periodically. You can set that up like this:

- Create a new policy. Under the **General** payload, set the trigger to **Recurring Check-in**, and the frequency to **Once every day**.
- Scroll down to the **Files and Process** payload, click **Configure**, and enter **sudo jamf policy -event epm-spectre** in the **Execute Command** field.

- Under the Scope tab, set the scope to All Computers (or whatever computers you prefer).

The **epm-spectre-force** trigger is a more aggressive version. It will install all updates immediately regardless of whether the applications are running, and it will install OS updates and reboot if necessary. Because this is potentially disruptive to users, it is recommended to only call this from Self Service policies with a clear description of what will happen. For example, you could set up such a policy like this:

- Create a new policy. Do *not* set a trigger in the General payload!
- Scroll down to the **Files and Process** payload, click **Configure**, and enter **sudo jamf policy -event epm-spectre-force** in the **Execute Command** field.
- Optional: under the **Restart Options** payload, you may change the delay before the computer restarts. The default is 5 minutes.
- Under the **Scope** tab, set the scope to All Computers (or whatever computers you prefer).
- Under the **Self Service** tab, check the **Make the policy available in Self Service** box.
- In the **Description** field, enter a note explaining to the user that the system may reboot and they should save all their work before proceeding. Check the **Ensure that users view the description** box.
- Optional: If you want the user to see this as soon as they open Self Service, check the **Feature the policy on the main page** box. If you do not check this box, the user will need to clic on the category for the policy on the right sidebar of Self Service.

You might need to run Apple software updates multiple times to be fully up to date. For example, if you're running macOS 10.13.1, you'll need to run it once to update to 10.13.3, then again to install the 10.13.3 Supplemental Update.

Contact

If you have questions or need assistance, contact the Endpoint Management team at epm-help@mit.edu.