New issue

Jump to bottom

Potential DoS for attacker that can create metadata files... #973

Closed JustinCappos opened this issue on Jan 8, 2020 · 2 comments

Assignees

Labels security

JustinCappos commented on Jan 8, 2020 • edited Member

We received the report below about an attacker that can create many invalid signatures on a metadata file, delaying the moment when the client will determine the signature is not valid. This delay may be for at least a few minutes, but possibly could be longer especially if multiple files are impacted.

Possible remediations include failing earlier (possibly immediately) if any signature is not valid.

Credit to Erik MacLean - Analog Devices, Inc. for reporting this issue.

(More Details below.)

Tracking ID: CVE-2020-6173

Summary:

Potential Client-side Denial of Service

Description:

While maximum file size is restricted for downloading, the client may attempt to validate a large number of signatures. We have been able to add over 500 copies of the same invalid signature into the `root.json` file, which results in the client attempting to validate each one, spending several minutes on validation. The file size limit of `target.json` is larger and may allow up to 5000 signatures, further increasing the amount of time spent in validation.

Security Impact: Denial of Service

Affected Version:

Identified at commit `9fde70f` , suspect all versions.

Credit:

Erik MacLean - Analog Devices, Inc.

JustinCappos assigned **mnm678** on Jan 8, 2020

JustinCappos added bug security labels on Jan 8, 2020

JustinCappos commented on Jan 8, 2020 Member Author

Because this seems like it will relate to crypto agility, I'd like **@mnm678** to take a look.

joshuagl commented on Sep 10, 2020 Member

This issue is now documented in advisory GHSA-2828-9vh6-9m6j

joshuagl closed this as completed on Sep 10, 2020

lukpueh removed the bug label on Sep 10, 2020

Assignees

mnm678

Labels

security

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

4 participants