Jump to bottom

Denial of Service in latest version [1.2.3] #52



New issue

⊙ Closed findneo opened this issue on Jan 19, 2020 · 7 comments · Fixed by #53

Assignees

findneo commented on Jan 19, 2020 • edited 🕶

Please confirm if it is vulnerable. Mitre id: CVF-2020-7226 Reporter: findneo

[Suggested description]

CiphertextHeader.java in

Cryptacular 1.2.3, as used in Apereo CAS and other products, allows attackers to trigger excessive memory allocation during a decode operation, because the nonce array length associated with "new byte" may depend on untrusted input within the header of encoded data.

[Additional Information]

any encoded network communication based on

org.cryptacular.CiphertextHeader#decode(byte[]) is affected. xxx of new byte[xxx] can be controlled by client and can be up to 0x7ffffffd ,which caused 2G of memory consuming without demanding for any

one of the products using this vuln code is cas4.2.0.

login flow of cas4.2.0 based on

org.cryptacular.CiphertextHeader#decode(byte[]) ,Concretely

speaking,the affected code is

org. jasig. spring. webflow. plugin. Encrypted Transcoder # decode

besides,codebase for cas4.2.0 is apereo/cas-overlay-template@ 7eaf9d7

[VulnerabilityType Other] Denial of Service

[Vendor of Product] http://www.cryptacular.org/

[Affected Product Code Base] cryptacular - 1.2.3

[Affected Component]

org.cryptacular.CiphertextHeader#decode(byte[]),

https://github.com/vt-middleware/cryptacular/blob/master/src/main/java/org/cryptacular/CiphertextHeader.java#L153

[Attack Type]

Remote

[Impact Denial of Service]

[Attack Vectors]

a crafted header of encoded data.

e.g '\x00\x00\x00\x34\x7f\xff\xff\xfd'

A garage description of the desc

serac commented on Jan 21, 2020

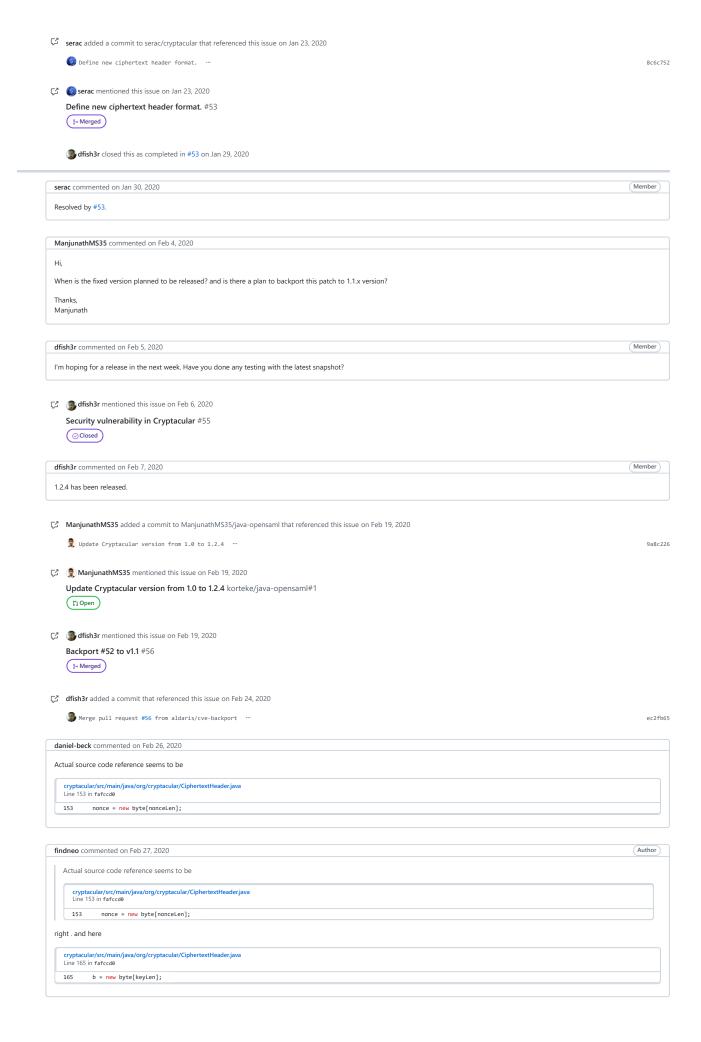
Member

Confirmed. We're analyzing feasibility of a backward-compatible patch and will follow up with release schedule shortly.

serac added a commit to serac/cryptacular that referenced this issue on Jan 23, 2020

WIP on backward compatible solution to vt-middleware#52.

dff3110



gnees
serac
els
e yet
ects
ie yet
estone
milestone
elopment
cessfully merging a pull request may close this issue.
Define new ciphertext header format. serac/cryptacular

5 participants

