

New issue

Jump to bottom

# Denial of Service in latest version [1.2.3] #52

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: [CVE-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 0x7fffffff  
,which caused 2G of memory consuming without demanding for any  
privilege.  
  
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.EncryptedTranscoder#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]  
true

[Attack Vectors]  
a crafted header of encoded data.  
e.g '\x00\x00\x00\x34\x7f\xff\xff\xfd'

dfish3r assigned serac on Jan 19, 2020

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.

df3110

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

 Define new ciphertext header format. ...

8c6c752

 **serac** mentioned this issue on Jan 23, 2020

Define new ciphertext header format. #53

 Merged

 **dfish3r** closed this as completed in #53 on Jan 29, 2020

**serac** commented on Jan 30, 2020

Member

Resolved by #53.

**ManjunathMS35** commented on Feb 4, 2020

Hi,

When is the fixed version planned to be released? and is there a plan to backport this patch to 1.1.x version?

Thanks,  
Manjunath

**dfish3r** commented on Feb 5, 2020

Member

I'm hoping for a release in the next week. Have you done any testing with the latest snapshot?

 **dfish3r** mentioned this issue on Feb 6, 2020

Security vulnerability in Cryptacular #55

 Closed

**dfish3r** commented on Feb 7, 2020

Member

1.2.4 has been released.

 **ManjunathMS35** added a commit to ManjunathMS35/java-opensaml that referenced this issue on Feb 19, 2020


 Update Cryptacular version from 1.0 to 1.2.4 ...

9a8c226

 **ManjunathMS35** mentioned this issue on Feb 19, 2020


Update Cryptacular version from 1.0 to 1.2.4 korteke/java-opensaml#1

 Open

 **dfish3r** mentioned this issue on Feb 19, 2020

Backport #52 to v1.1 #56

 Merged

 **dfish3r** added a commit that referenced this issue on Feb 24, 2020

 Merge pull request #56 from aldaris/cve-backport ...

ec2fb65

**daniel-beck** commented on Feb 26, 2020

Actual source code reference seems to be

[cryptacular/src/main/java/org/cryptacular/CiphertextHeader.java](#)  
Line 153 in fafccd0

```
153     nonce = new byte[nonceLen];
```

**findneo** commented on Feb 27, 2020

Author

Actual source code reference seems to be

[cryptacular/src/main/java/org/cryptacular/CiphertextHeader.java](#)  
Line 153 in fafccd0

```
153     nonce = new byte[nonceLen];
```

right . and here

[cryptacular/src/main/java/org/cryptacular/CiphertextHeader.java](#)  
Line 165 in fafccd0

```
165     b = new byte[keyLen];
```

Assignees



Labels

None yet

Projects


None yet

Milestone

No milestone

Development

Successfully merging a pull request may close this issue.

 Define new ciphertext header format.  
serac/cryptacular

5 participants

