[CVE-2020-13426] WORDPRESS PLUGIN MULTI-SCHEDULER 1.0.0 – CROSS-SITE REQUEST FORGERY

El mes pasado me dio por retomar un pasatiempo que me entretiene bastante, es la búsqueda de *bug* o fallos de seguridad en aplicaciones y recursos web. Esto me lo tomo con bastante calma y a diferencia de lo que son los programas de *Bug Bounty* y las competiciones de *CTF*, aquí no hay carrera por llegar el primero. Además también me lo tomo como un modo más de entrenamiento en mi continua formación. Ahora bien, hay que tener mucho cuidado con lo que se intenta evaluar ya que aquí podemos fácilmente cruzar la línea de la legalidad. Partimos desde la lógica de estar tocando un sistema o un activo que nadie nos ha pedido evaluar, por tanto esto siempre puede llevar a mal entendidos y situaciones adversas para nosotros como evaluadores. Para no tener que estar ganándome problemas innecesarios, yo me centro por lo general en la evaluación de aplicativos de software libre; En los *plugins* de *WordPress* tenemos bastante terreno por recorrer. ¿Qué nos hace falta para arrancar con todo esto? Pues básicamente el *plugin* y un entorno donde desplegar nuestro laboratorio con este CMS *WordPress*.

Vulnerabilidad CVE-2020-13426

Lo que vengo a presentar hoy es una vulnerabilidad básica de Cross-Site Request Forgery, también ubicada con las siglas *CSRF* en el plugin Multi-Scheduler de *WordPress*.

Básicamente podríamos definir *CSRF* como un ataque a través del cual podemos forzar al usuario autenticado a realizar una acción peligrosa y/o no deseada sobre el aplicativo web. Para esta vulnerabilidad concreta y como *prueba de concepto* (*PoC*) se evidencia como es posible eliminar registros (de la tabla "*professional*") en el aplicativo web, sin el consentimiento expreso del usuario final.

Multi-Scheduler se trata de un *plugin* que permite gestionar reservas de eventos (citas, reuniones, entrevistas...), manejando para ello un calendario de fechas, un listado de usuarios, listado de direcciones y la generación de reportes.

En la evaluación se evidencio que los formularios que permiten la eliminación y la creación de usuarios no cuenta con mecanismos *anti-CSRF*, es decir existe carencia en el uso de *tokens* para estos propósitos, depositando toda la confianza en la acción del usuario final, una acción que puede desatar terribles consecuencia como se observa en la PoC.

```
POST /wordpress/wp-admin/admin.php?page=msbdt_professional HTTP/1.1
Host: 192.168.122.181
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer:
http://192.168.122.181/wordpress/wp-admin/admin.php?page=msbdt_professional
Content-Type: application/x-www-form-urlencoded
Content-Length: 44
Cookie:
[redacted]
DNT: 1
Connection: close
Upgrade-Insecure-Requests: 1

pro_delete_id=920&professional_delete=Delete
```

Prueba de concepto (PoC)

Para poder demostrar la vulnerabilidad y su impacto se realizó la siguiente *PoC* que fue enviada al proveedor, en la cual se observa como es posible generar un formulario especialmente diseñado que puede ser enviado a la víctima para que la acción maliciosa (la eliminación de usuario) sea ejecutada en el aplicativo web.

agosto 2022
julio 2022
junio 2022
mayo 2022
abril 2022
marzo 2022
agosto 2021
julio 2021
junio 2021
mayo 2021
octubre 2020
septiembre 2020
agosto 2020
julio 2020
junio 2020
mayo 2020
abril 2020
septiembre 2019
febrero 2019
agosto 2018
mayo 2018
febrero 2018
junio 2017

Timeline

- **2020/05/21:** Descubrimiento de la vulnerabilidad
- **2020/05/22:** Notificación al proveedor
- **2020/05/23:** Solicitud de CVE a MITRE
- **2020/05/23:** Obtención del CVE por parte de MITRE
- **2020/06/20:** Publicación de la vulnerabilidad

Referencias

- **CVE MITRE:** https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-13426
- **Exploit Database:** https://www.exploit-db.com/exploits/48532
- **Packet Storm:** https://packetstormsecurity.com/files/157867/WordPress-Multi-Scheduler-1.0.0-Cross-Site-Request-Forgery.html
- **CXSecurity:** https://cxsecurity.com/issue/WLB-2020050235
- **0day Today:** https://0day.today/exploit/34496
- **Research Labs:** https://research-labs.net/search/exploits/wordpress-plugin-multi-scheduler-100-cross-site-request-forgery-delete-user