BOLETÍN DE ALERTA

Boletín Nro.: 2023-14
Fecha de publicación: 12/04/2023
Tema: Explotación activa de vulnerabilidad C*ross-Site scripting (XSS)* en Zimbra.

Software afectado:

- Zimbra Collaboration (ZCS), versión 9.0.

Descripción:

Se ha reportado un aviso de seguridad sobre una vulnerabilidad explotada activamente que afecta a Zimbra 9 que permite la utilización de una novedosa técnica de *phishing*, que permitiría a un atacante remoto no autenticado realizar ataques del tipo C*ross-Site Scripting Reflejado* (*XSS*) utilizando el web mail del servidor Zimbra vulnerable. Si bien esta vulnerabilidad no es considerada como *0-day*, existen muchos servidores que continúan desactualizados y pueden verse afectados por este ataque.

La vulnerabilidad identificada como CVE-2022-27926, de severidad "Media" y con puntuación asignada de 6.1. Esta vulnerabilidad del tipo *cross-site scripting (XSS*) se debe a una falla de validación de entradas del usuario en el componente *launchNewWindow.jsp* de Zimbra Collaboration. Esto permitiría a un atacante no autenticado a través de los de peticiones *HTTP* especialmente diseñadas, ejecutar códigos *JavaScript* arbitrarios en el navegador de las víctimas que visiten el sitio web afectado.

Impacto:

La explotación exitosa de esta vulnerabilidad permitiría a un atacante no autenticado realizar ataques del tipo *cross-site scripting (XSS)* a través del sitio web afectado.

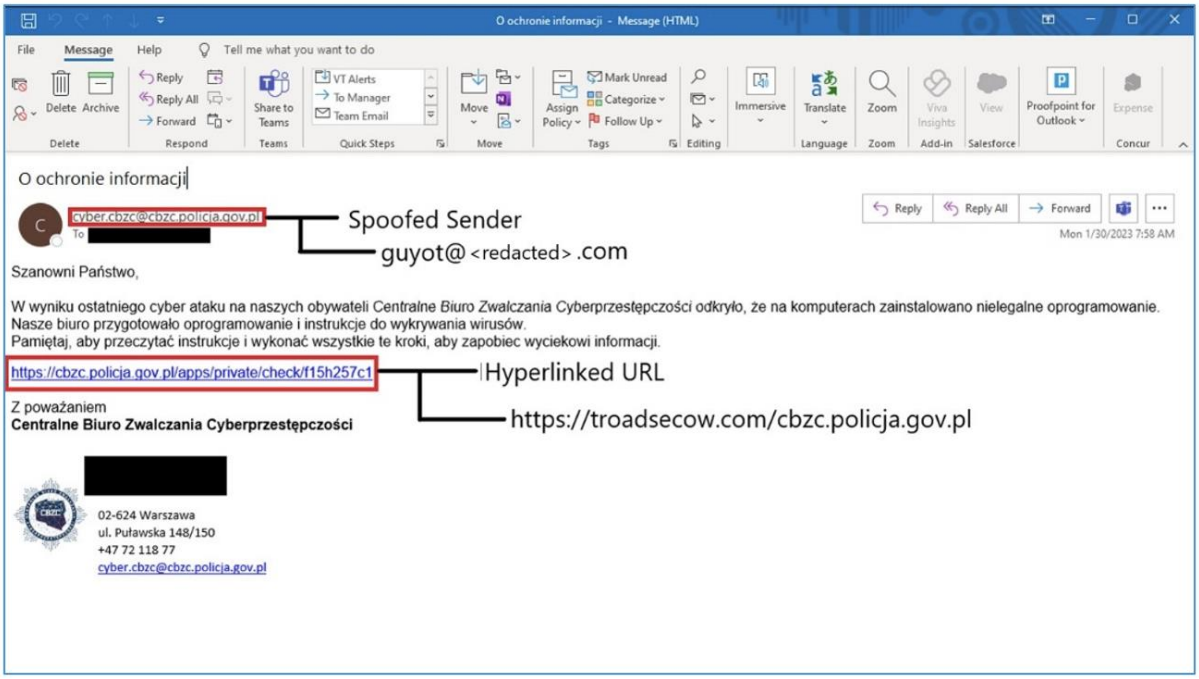
Novedosa técnica de phishing que explota la vulnerabilidad CVE-2022-27926:

Desde principios de 2023 esta vulnerabilidad CVE-2022-27926 está siendo explotada activamente por atacantes, principalmente contra organizaciones de gobierno, militares y diplomáticas, a través de campañas de *phishing* dirigidas a correos electrónicos. Permitiendo a través de esto: nuevas técnicas de recolección de credenciales, ejecución de ataques de instalación de *malware* y del tipo *cross-site request forgery* (*CSRF*).

A continuación, se detallan los pasos de la nueva técnica de phishing:

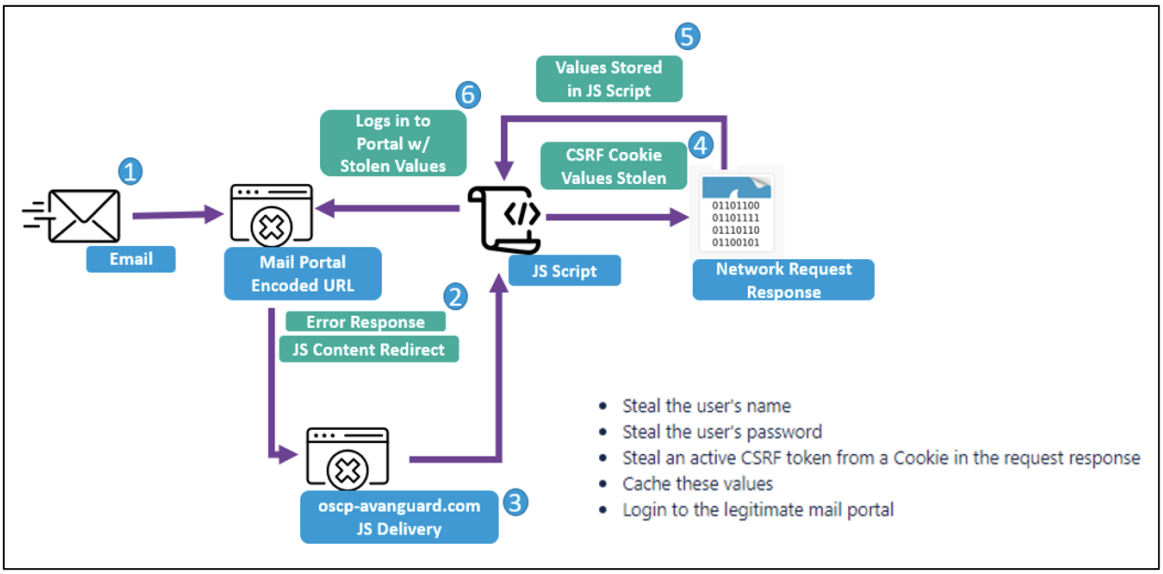
1. Envío de correos electrónicos desde direcciones de correo electrónico comprometidas.
2. Falsificación del campo remitente en el correo electrónico (también llamado *Spoofing*) para que aparezca como usuario de la organización de destino o bien, que aparezca como una organización involucrada en políticas globales.

3. Se incluye una *URL* auténtica de la organización de destino u organización relacionada relevante en el cuerpo del correo electrónico.
4. Se realiza un hipervínculo a la URL legitima - reconocida por la víctima - una *URL* maliciosa que apunta a una infraestructura controlada por el atacante y/o una URL legitima construida de tal forma que explote la vulnerabilidad CVE-2022-27926 para la entrega de un script en JavaScript (*payload*) que se ejecutaría en el navegador de la víctima, además los atacantes pueden redirigir a la víctima a una página de *phishing* para recolección de credenciales.
5. Se utilizan rutas de *URI* estructuradas que contienen un valor *hash* para la víctima, una indicación no codificada de la organización víctima y, en algunos casos, versiones codificadas o en texto plano de la *URL* legitima maliciosa que contenía el hipervínculo en el correo electrónico inicial enviada a las víctimas.



Fuente: https://www.proofpoint.com/us/blog/threat-insight/exploitation-dish-best-served-cold-winter-vivern-uses-known-zimbra-vulnerability

A continuación, se puede observar el proceso de infección de CSRF



Fuente: https://www.proofpoint.com/us/blog/threat-insight/exploitation-dish-best-served-cold-winter-vivern-uses-known-zimbra-vulnerability

Prevención:

Ante el incremento continuo de campañas de *phishing* alentamos a tener en cuenta varias medidas de prevención a seguir, indicadas en los siguientes enlaces que hemos publicado anteriormente:

- https://www.cert.gov.py/noticias/tecnica-de-phishing-en-adjuntos-html/
- https://www.cert.gov.py/wp-content/uploads/2022/12/GUIA-Configuracion-del-servidor-Zimbra_final3.pdf

Nota: Debido a la complejidad en la detección de estos tipos de ataques, si ve correos que apunten al web email de su organización, sugerimos consultar siempre la veracidad del correo recibido.

Solución:

Recomendamos mantener el sistema de correos Zimbra actualizado a la última versión disponible provista por el fabricante, pueden consultar las ultimas actualizaciones en el siguiente enlace:

- https://wiki.zimbra.com/wiki/Security_Center
- https://wiki.zimbra.com/wiki/Zimbra_Security_Advisories
- https://wiki.zimbra.com/wiki/Zimbra_Releases/9.0.0/P24

Información adicional:

- https://www.proofpoint.com/us/blog/threat-insight/exploitation-dish-best-served-cold-winter-vivern-uses-known-zimbra-vulnerability
- https://www.techrepublic.com/article/phishing-ta473-us-nato-officials/
- https://www.bleepingcomputer.com/news/security/winter-vivern-hackers-exploit-zimbra-flaw-to-steal-nato-emails/
- https://www.bleepingcomputer.com/news/security/cisa-warns-of-zimbra-bug-exploited-in-attacks-against-nato-countries/
- https://nvd.nist.gov/vuln/detail/CVE-2022-27926
- https://wiki.zimbra.com/wiki/Security_Center
- https://www.cert.gov.py/noticias/tecnica-de-phishing-en-adjuntos-html/
- https://www.cert.gov.py/wp-content/uploads/2022/12/GUIA-Configuracion-del-servidor-Zimbra_final3.pdf