Alerta de seguridad informática	9VSA-00094-001
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	2 de diciembre de 2019
Última revisión	2 de diciembre de 2019

NOTIFICACIÓN

La información consignada en el presente informe es producto del análisis de múltiples fuentes, de terceras partes, del propio fabricante e investigación propia del equipo CSIRT. La información contenida en los informes o comunicados está afecta a actualizaciones.

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte información obtenida del sitio oficial de Squid, referente a vulnerabilidades que afectan a sus servidores Proxy, las cuales, si son explotadas, pueden resultar en ataques de denegación de servicios, exposición de información y hasta ejecución de código remoto. Esto junto a su respectiva actualización para mitigar los riesgos.

Vulnerabilidad

- CVE-2019-12526
- CVE-2019-12523
- CVE-2019-18676
- CVE-2019-18677
- CVE-2019-18678
- CVE-2019-18679

Impacto

CVE-2019-12526.
Permite a un atacante remoto enviar grandes cantidades de datos arbitrarios en la pila, lo que puede llevar a una ejecución de código remoto. En sistemas con protección de acceso a la memoria, la explotación de esta vulnerabilidad mataría el proceso Squid, generando una denegación de servicios para los usuarios utilizando el proxy.

Producto Afectado

Squid 3.x hasta 3.5.28 (incluida).
Squid 4.x hasta 4.8 (incluida).

Mitigación

Se debe actualizar a la versión 4.9.

Enlaces

- http://www.squid-cache.org/Advisories/
- http://www.squid-cache.org/Advisories/SQUID-2019_7.txt
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=2019-12526

Impacto

CVE-2019-12523, CVE-2019-18676.
Debido a la falta de sanitización de inputs, existe una vulnerabilidad de tipo bypass, la cual permite a un atacante obtener acceso a servidores HTTP restringidos, también existe una vulnerabilidad de tipo desbordamiento de búfer en memoria, que permite a un atacante generar ataques de denegación de servicios para todos los usuarios utilizando el proxy.

Producto Afectado

Squid 3.x hasta 3.5.28 (incluida).
Squid 4.x hasta 4.8 (incluida).

Mitigación

Se debe actualizar a la versión 4.9.

Enlaces

- http://www.squid-cache.org/Advisories/
- http://www.squid-cache.org/Advisories/SQUID-2019_8.txt
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=2019-12523
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=2019-18676

Impacto

CVE-2019-18677.
Debido a un deficiente procesamiento de mensajes de Squid configurado con append_domain, se podría redirigir inapropiadamente el tráfico a orígenes que no debiesen recibirlo. Esto podría permitir a un atacante ocultar el server de origen para ataques phishing o URLs de descarga de malware.

Producto Afectado

Squid 2.x hasta 2.7.STABLE9 (incluida).
Squid 3.x hasta 3.5.28 (incluida).
Squid 4.x hasta 4.8 (incluida).

Mitigación

Se debe actualizar a la versión 4.9.

Enlaces

- http://www.squid-cache.org/Advisories/
- http://www.squid-cache.org/Advisories/SQUID-2019_9.txt
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=2019-18677

Impacto

CVE-2019-18678.
Debido a una vulnerabilidad de división de solicitud HTTP, causada por una incorrecta gestión de mensajes, un atacante podría interceptar solicitudes HTTP para corromper el caché entre el cliente y el servidor Squid.

Producto Afectado

Squid 3.x hasta 3.5.28 (incluida).
Squid 4.x hasta 4.8 (incluida).

Mitigación

Se debe actualizar a la versión 4.9.

Enlaces

- http://www.squid-cache.org/Advisories/
- http://www.squid-cache.org/Advisories/SQUID-2019_10.txt
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=2019-18678

Impacto

CVE-2019-18679
Debido a un error en la gestión de datos, Squid podría exponer información al procesar la autenticación HTTP que debilita la protección ASLR, ya que muestra un token Nonce. Estos tokens contienen el valor de un puntero que puede ayudar al atacante a aislar áreas de memoria para implementar ataques de ejecución de código remoto.

Producto Afectado

Squid 2.x hasta 2.7.STABLE9 (incluida).
Squid 3.x hasta 3.5.28 (incluida).
Squid 4.x hasta 4.8 (incluida).

Mitigación

Se debe actualizar a la versión 4.9.

Enlaces

- http://www.squid-cache.org/Advisories/
- http://www.squid-cache.org/Advisories/SQUID-2019_11.txt
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=2019-18679

CSIRT Gobierno de Chile
Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2019.12.02 13:26:28 -03'00'