Alerta de seguridad cibernética	9VSA20-00299-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	14 de septiembre de 2020
Última revisión	14 de septiembre de 2020

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 la información obtenida del GitHub oficial de Squid respecto a tres vulnerabilidades que afectan a sus servidores Proxy. El presente informe incluye medidas de mitigación.

Vulnerabilidades

CVE-2020-15810
CVE-2020-15811

CVE-2020-15810

Debido a la incorrecta validación de datos ingresados por un usuario, es posible realizar un ataque de envenenamiento de caché debido a que el tráfico HTTP y HTTPS puede ser vandalizado por terceros. Este problema grave permite a cualquier cliente, incluido scripts del navegador, evitar la seguridad local y envenenar el caché del navegador y cualquier otro caché downstream con contenido de una fuente arbitraria.

Productos Afectados
Squid versiones 2.5-3.5.28, 4.0-4.12 y 5.0.1-5.0.

Mitigaciones
Se debe actualizar a las versiones 4.13 y 5.0.4 para resolver la vulnerabilidad.

Enlaces
https://github.com/squid-cache/squid/security/advisories/GHSA-3365-q9qx-f98m/
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-15810

CVE-2020-15811

Debido a la incorrecta validación de datos ingresados por un usuario, es posible realizar un ataque de envenenamiento de caché debido a que el tráfico HTTP y HTTPS puede ser dividido por terceros. Este problema grave permite a cualquier cliente, incluido scripts del navegador, evitar la seguridad local y envenenar el caché del proxy y cualquier otro caché downstream con contenido de una fuente arbitraria.

Productos Afectados
Squid versiones 2 2.7-3.5.28, 4.0-4.12 y 5.0.1-5.0.3

Mitigaciones
Se debe actualizar a las versiones 4.13 y 5.0.4 para resolver la vulnerabilidad.

Enlaces
https://github.com/squid-cache/squid/security/advisories/GHSA-c7p8-xqhm-49wv/
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-15811