Alerta de seguridad cibernética	9VSA20-00262-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	08 de julio de 2020
Última revisión	08 de julio 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 la respectiva medida de mitigación.

Vulnerabilidades

CVE-2020-14059
CVE-2020-14058
CVE-2020-15049

CVE-2020-14059

Debido a una incorrecta sincronización al procesar objetos en el cache SMP, un cliente remoto podría gatillar un “squid worker assertion” y causar una denegación de servicios. Este ataque está limitado a Squid SMP que utilice memoria caché compartida y/o un caché de disco de roca SMP.

Productos Afectados
Squid versiones 5.0.1-5.0.2.

Mitigación
Actualizar a la versión 5.0.3 de Squid.

Enlaces
https://github.com/squid-cache/squid/security/advisories/GHSA-w7pw-2m4p-58hr
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-14059

CVE-2020-14058

Debido al uso de funciones potencialmente peligrosas al procesar certificados TLS, un cliente remoto podría causar una denegación de servicios al abrir conexiones TLS.

Productos Afectados
Squid versiones 3.1-3.5.28, 4.0-4.11, 5.0.1-5.0.2.

Mitigación
Actualizar a la versión 4.12 o 5.0.3 de Squid.

Enlaces
https://github.com/squid-cache/squid/security/advisories/GHSA-qvf6-485q-vm57
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-14058

CVE-2020-15049

Debido a la forma en que Squid procesa las peticiones de clientes, un cliente remoto podría enviar datos especialmente diseñados en la petición para realizar el contrabando de solicitudes y envenenar los contenidos del caché HTTP con mensajes HTTP especialmente diseñados.
Como condición para explotar la vulnerabilidad, se requiere que un Upstream server sea quien la secuencia de respuesta envenenada.

Productos Afectados

Squid versiones 2.0-2.STABLE9, 3.0-3.5.28, 4.0-4.11, 5.0.1-5.0.2.

Mitigación

Actualizar a la versión 4.12 o 5.0.3 de Squid.

Enlaces

https://github.com/squid-cache/squid/security/advisories/GHSA-qf3v-rc95-96j5
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-15049