Alerta de Seguridad Cibernética

Alerta de seguridad cibernética	9VSA20-00287-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	20 de agosto de 2020
Última revisión	20 de agosto de 2020

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte la información obtenida de Jenkins respecto a una vulnerabilidad que permitiría la filtración de datos HTTP sensibles por causa del uso de Jetty vulnerable. El presente informe incluye la respectiva medida de mitigación.

Vulnerabilidad

CVE-2019-17638

Impacto

Jenkins utiliza Jetty 9.4.27 el cual contiene una vulnerabilidad que permitiría a atacantes no autenticados obtener encabezados de respuesta HTTP que podrían incluir datos sensibles destinados a otros usuarios.
En el caso de que estos encabezados de respuesta sean muy largos, Jetty arroja una excepción generando el código de error HTTP 431. Cuando esto sucede, el "ByteBuffer" que contiene el encabezado de respuesta, es enviado devuelta al "ByteBufferPool" dos veces. A causa de esto, dos subprocesos adquieren el mismo "ByteBuffer" del grupo, y mientras el "hilo 1" está a punto de utilizar "ByteBuffer" para escribir los datos de respuesta en "respuesta 1", el "hilo 2" sobreescribe el "ByteBuffer" con los datos de "respuesta 2". "Hilo 1" finalmente queda con los datos de "respuesta 2", resultando en que el cliente 1 recibida la respuesta HTTP del cliente 2 (ID de sesiones HTTP, credenciales de autenticación, etc.) .

Productos Afectados

Jenkins weekly versión 2.242 y anteriores.
Jenkins LTS versión 2.235.4 y anteriores

Mitigaciones

Jenkins weekly debe ser actualizado a la versión 2.243.
Jenkins LTS debe ser actualizado a la versión 2.235.5.

Enlaces

https://www.jenkins.io/security/advisory/2020-08-17/
https://github.com/advisories/GHSA-x3rh-m7vp-35f2
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-17638

CSIRT Gobierno de Chile
Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2020.08.20 19:27:56 -04'00'