Alerta de Seguridad Cibernética

Alerta de seguridad cibernética	9VSA20-00327-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	24 de noviembre de 2020
Última revisión	24 de noviembre 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 de Drupal referente a vulnerabilidad que permitiría la ejecución de código remoto mediante archivos no sanitizados. El presente informe incluye la respectiva medida de mitigación.

Vulnerabilidad

CVE-2020-13671

CVE-2020-13671

Drupal core no sanitiza correctamente algunos nombres de archivo o archivos cargados, lo cual podría llevar a que ciertos archivos sean interpretados con la extensión incorrecta, siendo utilizados con el tipo de MIME incorrecto o ejecutando código PHP para ciertas configuraciones de host.

Productos Afectados

Drupal versiones 9.x, 8.9.x, 8.8.x y anteriores y 7.x y anteriores.

Mitigación

Actualizar a la versión 9.0.8, 8.9.9, 8.8.11 o 7.74 de Drupal.
Además se recomienda revisar todos los archivos previamente cargados en busca de extensiones maliciosas. Especialmente archivos con dos extensiones como "file.php.txt" o "file.html.gif", que no tengan un guion bajo (_) en la extensión.
Se recomienda prestar especial atención a las extensiones phar, php, pl, py, cgi, asp, js, html, htm y phtml.

Enlaces

https://www.drupal.org/sa-core-2020-012
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-13671

CSIRT Gobierno de Chile
Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2020.11.24 08:44:48 -03'00'