Alerta de seguridad cibernética	9VSA20-00247-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	19 de junio de 2020
Última revisión	19 de junio 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 tres vulnerabilidades que afectan a su Gestor de contenidos web. El presente informe incluye la respectiva medida de mitigación.

Vulnerabilidades

CVE-2020-13663
CVE-2020-13664
CVE-2020-13665

CVE-2020-13663

Debido a que el formulario API de Drupal core no valida correctamente ciertos datos ingresados por un usuario, un atacante podría explotar la vulnerabilidad de tipo Cross Site Request Forgery (CSRF) enviando peticiones a otros servicios desde el formulario, lo cual le permitiría explotar otras vulnerabilidades.
Impacto: crítico.

Productos Afectados
Drupal versiones 7.x, 8.x y 9.x.

Mitigación
Para la versión 7.x, actualizar a la 7.72.
Para la versión 8.8.x, actualizar a la versión 8.8.8.
Para la versión 8.9.x, actualizar a la versión 8.9.1.
Para la versión 9.0.x, actualizar a la versión 9.0.1.
Ya no existe soporte para las versiones entre la 8 y la 8.8.x, por lo que se recomienda actualizar a la versión 8.8.8.

Enlaces
https://www.drupal.org/sa-core-2020-004
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-13663

CVE-2020-13664

Un atacante podría engañar a un Administrador que utilice Windows para que visite un sitio malicioso, lo cual resultaría en la creación de un directorio cuidadosamente creado en el sistema de archivos. Con este directorio, el atacante podría intentar explotar una vulnerabilidad de ejecución de código PHP remoto a través de fuerza bruta.
Impacto: crítico.

Productos Afectados
Drupal versiones 8.x y 9.x.

Mitigación
Para la versión 8.8.x, actualizar a la versión 8.8.8.
Para la versión 8.9.x, actualizar a la versión 8.9.1.
Para la versión 9.0.x, actualizar a la versión 9.0.1.
Ya no existe soporte para las versiones entre la 8 y la 8.8.x, por lo que se recomienda actualizar a la versión 8.8.8.

Enlaces
https://www.drupal.org/sa-core-2020-005
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-13664

CVE-2020-13665

Peticiones JSON:API Patch podrían evadir validaciones en ciertos campos permitiendo a un atacante enviar peticiones especialmente diseñadas para causar una denegación de servicios en el sistema afectado.
Por defecto JSON:API solo funciona en modo lectura, por lo que se tendría que modificar "jsonapi.settings" para que la vulnerabilidad esté presente.

Productos Afectados

Drupal versiones 8.x y 9.x.

Mitigación

Para la versión 8.8.x, actualizar a la versión 8.8.8.
Para la versión 8.9.x, actualizar a la versión 8.9.1.
Para la versión 9.0.x, actualizar a la versión 9.0.1.
Ya no existe soporte para las versiones entre la 8 y la 8.8.x, por lo que se recomienda actualizar a la versión 8.8.8.

Enlaces

https://www.drupal.org/sa-core-2020-006
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-13665

CSIRT Gobierno de Chile
Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2020.06.19 00:02:06 -04'00'