Alerta de seguridad cibernética	9VSA20-00197-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	30 de abril de 2020
Última revisión	30 de abril 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 entregada por Adobe referente a múltiples vulnerabilidades que afectan a su producto Magento. El presente informe incluye la respectiva medida de mitigación.

VULNERABILIDADES

CVE-2020-9576
CVE-2020-9577
CVE-2020-9578
CVE-2020-9579
CVE-2020-9580
CVE-2020-9581
CVE-2020-9582
CVE-2020-9583
CVE-2020-9584
CVE-2020-9585
CVE-2020-9587
CVE-2020-9588
CVE-2020-9591

CVE-2020-9576, CVE-2020-9578, CVE-2020-9582 CVE-2020-9583

Debido a que no se valida correctamente los datos ingresados por usuarios, un atacante remoto y autenticado como administrador podría inyectar comandos de OS arbitrarios al sistema.

CVE-2020-9577, CVE-2020-9581, CVE-2020-9584

Debido a la insuficiente sanitización de datos ingresados por el usuario, un atacante remoto no autenticado podría inyectar y ejecutar permanentemente código script y HTML en el contexto del sitio vulnerable. La explotación exitosa de esta vulnerabilidad XSS (Cross-site scripting) permitiría al atacante modificar el contenido del sitio web, robar información potencialmente sensible y engañar a la víctima para que descargue malware.

CVE-2020-9579, CVE-2020-9580, CVE-2020-9585

Debido a que no se valida correctamente los datos ingresados por usuarios, un atacante remoto y autenticado como administrador podría inyectar comandos arbitrarios al sistema vulnerable.

CVE-2020-9587

Existe un error no especificado por Adobe, que permitiría a un atacante remoto no autenticado obtener acceso a descuentos de productos que normalmente no estarían disponibles.

CVE-2020-9588

Existe un error no especificado por Adobe, que permitiría a un atacante remoto autenticado como administrador evadir ciertas restricciones de seguridad implementadas.

CVE-2020-9591

Existe un error que permitiría a un atacante remoto no autenticado obtener acceso a la interfaz con el panel de administrador.

PRODUCTOS AFECTADOS

Magento Commerce versiones 2.3.4 y anteriores.
Magento Open Source versiones 2.3.4 y anteriores

Magento Commerce versiones 2.2.11 y anteriores.
Magento Open Source versiones 2.2.11 y anteriores.

Magento Enterprise Edition versiones 1.14.4.4 y anteriores.
Magento Community Edition versiones 1.9.4.4 y anteriores.

MITIGACIÓN

Para Magento Commerce actualizar a la versión 2.3.4-p2.
Para Magento Open Source actualizar a la versión 2.3.4-p2.

Para Magento Commerce actualizar a la versión 2.3.5-p1.
Para Magento Open Source actualizar a la versión 2.3.5-p1.

Para Magento Enterprise Edition actualizar a la versión 1.14.4.5.
Para Magento Community Edition actualizar a la versión 1.9.4.5.

Enlaces
https://helpx.adobe.com/security/products/magento/apsb20-22.html
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9576
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9577
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9578
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9579
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9580
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9581
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9582
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9583
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9584
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9585
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9587
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9588
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9591

CSIRT Gobierno de Chile
Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2020.04.30 12:22:41 -04'00'