| | |
|---|---|
| Alerta de seguridad informática | 9VSA20-00149-01 |
| Clase de alerta | Vulnerabilidad |
| Tipo de incidente | Sistema y/o Software Abierto |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 28 de Febrero de 2020 |
| Última revisión | 28 de Febrero 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 información obtenida del repositorio oficial de MISP, referente a múltiples vulnerabilidades que afectan a su plataforma, las cuales permitirían a un atacante remoto realizar ataques XSS, obtener acceso a funcionalidades no autorizadas, evadir medidas de seguridad y realizar ataques de fuerza bruta. Este informe incluye su respectiva mitigación.

## Vulnerabilidades

CVE-2020-8890

CVE-2020-8891

CVE-2020-8892

CVE-2020-8893

CVE-2020-8894

### Impacto
CVE-2020-8890
Debido a una incorrecta medida de protección ante ataques de fuerza bruta, un atacante remoto podría causar que la aplicación de base de datos responda lento a las peticiones y utilizar esta situación para evadir la protección de fuerza bruta.

### Producto Afectado
MISP entre las versiones 2.4.51 hasta la 2.4.120.

### Impacto
CVE-2020-8891
Debido a que la aplicación no canoniza los nombres de usuarios al intentar bloquear series de peticiones inválidas en ataques de fuerza bruta, un atacante remoto podría evadir este mecanismo de seguridad y aún así realizar ataques de fuerza bruta.

### Producto Afectado
MISP entre las versiones 2.4.51 hasta la 2.4.120.

### Impacto
CVE-2020-8892
Debido a que la aplicación no considera la posibilidad de usar el método HTTP PUT al intentar bloquear series de peticiones inválidas en ataques de fuerza bruta, un atacante remoto podría evadir este mecanismo de seguridad utilizando el método PUT para así realizar ataques de fuerza bruta.

### Producto Afectado
MISP versiones 0.1, 0.2, 2.1, 2.1.18, 2.2.1, 2.2.2, entre la versión 2.3.0 hasta la 2.3.178 y desde la versión 2.4.0 hasta la 2.4.120.

### Impacto
CVE-2020-8893
Esta vulnerabilidad permite a un atacante remoto realizar ataques XSS (Cross-site Scripting) debido a la insuficiente sanitización de datos ingresados por el usuario en “app/View/Galaxies/view.ctp“. El atacante podría enviarle a la víctima un sitio web especialmente diseñado para que ejecute HTML arbitrario y código script en el navegador del usuario. Esto le permitiría robar información potencialmente sensible, cambiar la apariencia de la página web, realizar ataques phishing y hasta forzarlo a descargar archivos maliciosos.

### Producto Afectado
MISP entre las versiones 2.4.94 hasta la 2.4.120.

## Impacto

CVE-2020-8894

Debido a restricciones de acceso inadecuadas en los scripts “app/Controller/ThreadsController.php” y “app/Model/Thread.php” un usuario autenticado podría evadir restricciones de seguridad y ver discusiones que normalmente no podría.

## Producto Afectado

MISP entre las versiones 2.4.0 hasta la 2.4.120.

## Mitigación

Actualizar a la versión 2.4.121.

## Enlaces

https://github.com/MISP/MISP/compare/v2.4.120...v2.4.121
https://github.com/MISP/MISP/commit/3d982d92fd26584115c01f8c560a688d1096b65c
https://github.com/MISP/MISP/commit/9400b8bc8699435d84508e598aca98a31affd77c
https://github.com/MISP/MISP/commit/934c82819237b4edf1da64587b72a87bec5dd520
https://github.com/MISP/MISP/commit/c1a0b3b2809b21b4df8c1efbc803aff700e262c3
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-8890
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-8891
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-8892
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-8893
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-8894

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2020.02.28 12:15:32 -03'00'