Alerta de seguridad cibernética	9VSA20-00217-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	20 de mayo de 2020
Última revisión	20 de mayo 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 MISP referente a vulnerabilidad que afecta a la plataforma para compartir información de malware. El presente informe incluye la respectiva medida de mitigación.

Vulnerabilidad

CVE-2020-13153

CVE-2020-13153

Debido a insuficiente sanitización de datos ingresados por el usuario en "app/View/Events/resolved_attributes.ctp", es posible para un atacante remoto realizar ataques XSS (Cross-site Scripting), al enviarle un enlace especialmente diseñado a una víctima, logrando ejecutar HTML y código JavaScript en el contexto del sitio vulnerable.
La explotación exitosa de esta vulnerabilidad permitiría al atacante robar información potencialmente sensible, cambiar la apariencia del sitio y engañar a la víctima para que descargue malware.

Producto Afectado

Esta vulnerabilidad afecta a todas las versiones de MISP.

Mitigación

Actualizar a la versión 2.4.126 de MISP.

Enlaces

https://github.com/MISP/MISP/compare/v2.4.125...v2.4.126
https://github.com/MISP/MISP/commit/2989aa05225aa9b3a592ca50cbf8350ef256909c
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-13153