Alerta de Seguridad Cibernética

Alerta de seguridad cibernética	9VSA21-00528-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	6 de diciembre de 2021
Última revisión	6 de diciembre de 2021

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 del Gobierno de Chile, CSIRT de Gobierno, comparte información sobre vulnerabilidades en IBM QRadar SIEM.

Este informe incluye las medidas de mitigación, consistentes en instalar la última actualización de los productos afectados.

Vulnerabilidades

CVE-2017-15713
CVE-2021-32399
CVE-2021-29650
CVE-2021-29154
CVE-2021-22555
CVE-2020-27777
CVE-2021-3715
CVE-2019-9924
CVE-2018-18751
CVE-2018-11768
CVE-2020-7226
CVE-2020-9492
CVE-2018-8029
CVE-2020-13954
CVE-2021-22696
CVE-2021-28163
CVE-2021-28169
CVE-2021-28165
CVE-2021-29425
CVE-2021-2161

Impactos

Vulnerabilidad grave

CVE-2018-8029: Esta vulnerabilidad permite a un atacante remoto escalar privilegios en el sistema afectado. La vulnerabilidad existe debido a restricciones de acceso inapropiadas a la interfaz de la API.

Productos afectados

IBM Qradar SIEM: 7.3.0 a 7.4.3 Fix Pack 2, 7.4.3 GA.

Mitigación

Instalar las respectivas actualizaciones entregadas por el proveedor.

Enlaces

https://www.ibm.com/blogs/psirt/security-bulletin-ibm-qradar-siem-is-vulnerable-to-using-components-with-known-vulnerabilities-12/
http://www.ibm.com/support/pages/node/6520472
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-15713
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-32399
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-29650
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-29154
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-22555
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-27777
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-3715
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-9924
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-18751
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-11768
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-7226
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9492
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-8029
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-13954
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-22696
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-28163
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-28169
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-28165
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-29425
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-2161

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2021.12.06 17:12:23 -03'00'