Alerta de seguridad cibernética	9VSA23-00895-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
TLP	Blanco
Fecha de lanzamiento original	8 de septiembre de 2023
Última revisión	8 de septiembre de 2023

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 CSIRT de Gobierno. La información contenida en los informes o comunicados está afecta a actualizaciones.

Resumen

El CSIRT de Gobierno comparte información de vulnerabilidades parchadas por Cisco para varios de sus productos.

Vulnerabilidades

CVE-2023-20238
CVE-2023-20193
CVE-2023-20194
CVE-2023-20243
CVE-2023-20250
CVE-2023-20263
CVE-2023-20269

Impacto

Vulnerabilidades de riesgo crítico

CVE-2023-20238: Vulnerabilidad en la implementación single sign-on (SSO) en Cisco BroadWorks Application Delivery Platform y Cisco BroadWorks Xtended Services Platform, que podría permitir a un atacante remoto y no autenticado falsificar las credenciales requeridas para accder a un sistema afectado.

Mitigación

Instalar las respectivas actualizaciones entregadas por el proveedor.

Productos afectados

Cisco BroadWorks Application Delivery Platform
Cisco BroadWorks Xtended Services Platform
Cisco Identity Services Engine (ISE)
Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers

Cisco HyperFlex HX Data Platform
Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software

Enlaces

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-bw-auth-bypass-kCggMWhX
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-radius-dos-W7cNn7gt
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-priv-esc-KJLp2Aw
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv-stack-SHYv2f5N
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-hyperflex-redirect-UxLgqdUF
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-ravpn-auth-8LyfCkeC
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-20238
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-20193
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-20194
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-20243
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-20250
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-20263
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-20269

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2023.09.08 14:21:39 -03'00'