Alerta de seguridad cibernética	9VSA21-00465-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	9 de julio de 2021
Última revisión	9 de julio 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 que afectan a diversos productos de Cisco.

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

Vulnerabilidades

CVE-2021-1562
CVE-2018-0155
CVE-2021-1359
CVE-2021-1574
CVE-2021-1576
CVE-2021-3449
CVE-2021-3450

Impactos

CVE-2021-1562 (riesgo medio): Esta vulnerabilidad en la interfaz XSI-Actions de Cisco BroadWorks Application Server podría permitir un usuario remoto autenticado acceder a información sensible en el sistema afectado.

CVE-2018-0155 (riesgo alto): Esta vulnerabilidad en la implementación offload de Bidirectional Forwarding Detection (BFD) en switches Cisco Catalyst 4500 Series y 4500-X Series podría permitir a un atacante remoto no autenticado generar un colapso de los procesos iosd.

CVE-2021-1359 (riesgo alto): Esta vulnerabilidad en la administración de configuración de Cisco AsyncOS para Cisco Web Security Appliance (WSA) podría permitir a un atacante remoto no autenticado realizar inyección de comandos y elevar privilegios a root.

CVE-2021-1574 y CVE-2021-1576 (riesgo alto): Estas vulnerabilidades en la interfaz web de Cisco Business Process Automation (BPA) podrían permitir a un atacante autenticado remoto a elevar privilegios a Administrador.

CVE-2021-3449 y CVE-2021-3450 (riesgo alto): Estas vulnerabilidades podrían permitir a un atacante usar un certificado que no corresponda a una autoridad certificadora como si lo fuera y firmar un certificado para una organización, usuario o aparato arbitrarios, o para causar una condición de denegación de servicio (DoS).

Productos Afectados

Cisco BroadWorks Application Server
Cisco Catalyst 4500 Series Switches
Cisco Catalyst 4500-X Series Switches
Cisco Web Security Appliance (WSA)

Mitigación

Instalar las respectivas actualizaciones desde el sitio web del proveedor.

Enlaces

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-broad-as-inf-disc-ZUXGFFXQ
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180328-bfd
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-scr-web-priv-esc-k3HCGJZ
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-bpa-priv-esc-dgubwbH4
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-openssl-2021-GHY28dJd
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1562
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-0155
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1359
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1574
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1576
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-3449
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-3450

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2021.07.09 19:30:40 -04'00'