Alerta de Seguridad Cibernética

Alerta de seguridad cibernética	9VSA21-00456-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Crítico
TLP	Blanco
Fecha de lanzamiento original	17 de junio de 2021
Última revisión	17 de junio 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 diversas vulnerabilidades que afectan a productos de Cisco.

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

Vulnerabilidades

CVE-2021-1242
CVE-2021-1568
CVE-2021-1395
CVE-2021-1569
CVE-2021-1570
CVE-2021-1524
CVE-2021-1567
CVE-2021-1541
CVE-2021-1542
CVE-2021-1543
CVE-2021-1571
CVE-2021-1134
CVE-2021-1566

Impactos

Vulnerabilidades de riesgo alto son las siguientes

CVE-2021-1567 afecta el mecanismo de carga de DLL en Cisco AnyConnect Secure Mobility Client para Windows, y podría permitir a un atacante local realizar ataques de secuestro de DLL en el aparato afectado, si está instalado el módulo VPN Posture (HostScan) en el cliente AnyConnect.

CVE-2021-1542: Esta vulnerabilidad en la interfaz de administración web de los Cisco Small Business 220 Series Smart Switches permite a un atacante remoto y no autenticado el evadir las protecciones de autenticación, ganando acceso no autorizado a la interfaz.

CVE-2021-1134: Esta vulnerabilidad en la funcionalidad de integración Cisco Identity Services Engine (ISE) del Cisco DNA Center permitiría a un atacante remoto no autenticado ganar acceso no autorizado a datos sensibles.

CVE-2021-1566: Esta vulnerabilidad en la integración de Cisco Advanced Malware Protection para Endpoints de Cisco AsyncOS para Cisco Email Security Appliance (ESA) y Cisco Web Security Appliance (WSA) podría permitir a un atacante remoto no autenticado el interceptar tráfico ente un aparato afectado y los servidores de AMP.

Productos Afectados

Cisco AnyConnect Secure Mobility
Cisco Jabber
Cisco Webex
Cisco AnyConnect
Cisco Unified Intelligence Center
Cisco Meeting Server API
Cisco Small Business 220 Series Smart Switches
Cisco DNA Center Software
Cisco Email Security Appliance
Cisco Web Security Appliance

Mitigación

Instalar las respectivas actualizaciones desde el sitio web del proveedor.

Enlaces

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-anyconnect-pos-dll-ff8j6dFv
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ciscosb-multivulns-Wwyb7s5E
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-dnac-certvalid-USEj2CZk
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1242
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1568
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1395
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1569
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1570
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1524
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1567
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1541
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1542
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1543
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1571
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1134
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1566

CSIRT Gobierno de Chile
Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2021.06.17 12:22:14 -04'00'