Alerta de seguridad cibernética	9VSA21-00426-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Crítico
TLP	Blanco
Fecha de lanzamiento original	21 de abril de 2021
Última revisión	21 de abril 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, CSIRT de Gobierno, comparte información sobre una nueva vulnerabilidad en Pulse Connect Secure.

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

Vulnerabilidad

CVE-2021-22893

Impactos

La vulnerabilidad permite evadir la autenticación y que un usuario no autenticado realice la ejecución remota de archivos arbitrarios en la puerta de enlace (gateway) de Pulse Connect Secure.

Productos Afectados

Pulse Connect Secure (PCS) 9.0R3 y superior.

Mitigación

Instalar las respectivas actualizaciones desde el sitio web del proveedor cuando estén disponibles.

Mientras tanto, el proveedor informa que la vulnerabilidad puede ser mitigada importando el archivo Workaround-2104[.]xml, el que es posible descargar en su web dedicada a la presente vulnerabilidad (https://kb.pulsesecure.net/articles/Pulse_Security_Advisories/SA44784/).

Los clientes de PCS también pueden importarlo desde la aplicación, yendo a

- Maintenance > Import/Export > Import XML.
- Esto desactiva Pulse Collaboration.
- Si hay un load balancer delante del PCS, esto puede afectar al Load Balancer.
- Si su load balancer está usando Round Robin, HealthCheck.cgi or Advanced healthcheck.cgi, no se verá afectado.

Desactive el Windows File Browser

- Navegue a User > User Role > Clic en Default Option >> Clic en General.
- Bajo Access Feature, asegúrese de que la opción "Files, Window" no esté seleccionada.
- Vaya a Users > User Roles.
- Haga clic en cada rol y asegúrese de que bajo Access Feature en cada rol, la opción File, Windows no esté activada.

No es necesario reiniciar los servicios bajo la appliance de Pulse Secure.

La URI son las siguientes, en el caso de que quiera bloquearlas en la frontera de su red:

^/+dana/+meeting
^/+dana/+fb/+smb
^/+dana-cached/+fb/+smb
^/+dana-ws/+namedusers
^/+dana-ws/+metric

El proveedor explica que esta mitigación debe ser removida cuando se aplique el parche respectivo.

Enlaces
https://kb.pulsesecure.net/articles/Pulse_Security_Advisories/SA44784/
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-22893

CSIRT Gobierno de Chile
Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2021.04.21 12:09:38 -04'00'