Alerta de seguridad cibernética	9VSA22-00730-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Crítico
TLP	Blanco
Fecha de lanzamiento original	20 de octubre de 2022
Última revisión	20 de octubre de 2022

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 Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT de Gobierno, comparte información sobre nuevas vulnerabilidades comunicadas por F5.

Vulnerabilidades

CVE-2022-36795
CVE-2022-41617
CVE-2022-41624
CVE-2022-41691
CVE-2022-41694
CVE-2022-41741
CVE-2022-41742
CVE-2022-41743
CVE-2022-41770
CVE-2022-41780
CVE-2022-41787
CVE-2022-41806
CVE-2022-41813
CVE-2022-41832
CVE-2022-41833
CVE-2022-41835
CVE-2022-41836
CVE-2022-41983

Impacto

Vulnerabilidades de riesgo crítico

CVE-2022-41617: Ejecución remota de código autenticado en la interfaz BIG-IP iControl REST.

Productos afectados

BIG-IP (Advanced WAF, ASM) 14.1.5
BIG-IP (Advanced WAF, ASM) 16.1.0 - 16.1.2
BIG-IP (Advanced WAF, ASM) 16.1.0 - 16.1.3
BIG-IP (Advanced WAF, ASM) 17.0.0
BIG-IP (AFM) 16.1.0 - 16.1.3
BIG-IP (AFM, PEM) 16.1.0 - 16.1.3
BIG-IP (todos los módulos) 13.1.0 - 13.1.5
BIG-IP (todos los módulos) 16.1.0 - 16.1.2
BIG-IP (todos los módulos) 16.1.0 - 16.1.3

BIG-IP (todos los módulos) 17.0.0
BIG-IP (DNS, LTM con licencia DNS Services) 17.0.0
BIG-IQ Centralized Management 8.0.0 - 8.2.0
F5OS-A 1.0.0 - 1.0.1
F5OS-C 1.1.0 - 1.3.2
F5OS-C 1.3.0 - 1.3.2
NGINX App Protect WAF 3.0.0 - 3.11.0
NGINX Ingress Controller 2.0.0 - 2.4.0
NGINX Open Source 1.23.0 - 1.23.1
NGINX Plus R22 - R27
R1 P1
R2 P1
R26 P1

Mitigación

Instalar las respectivas actualizaciones entregadas por el proveedor.

Enlaces

https://support.f5.com/csp/article/K30425568
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-36795
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-41617
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-41624
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-41691
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-41694
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-41741
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-41742
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-41743
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-41770
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-41780
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-41787
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-41806
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-41813
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-41832
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-41833
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-41835
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-41836
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-41983

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2022.10.21 11:32:01 -03'00'