BOLETÍN DE ALERTA

Boletín Nro.: 2022-49
Fecha de publicación: 10/11/2022
Tema: Vulnerabilidades graves en Citrix Gateway y Citrix ADC.

Los productos afectados son:

- Citrix ADC and Citrix Gateway 13.1, versiones anteriores a 13.1-33.47.
- Citrix ADC and Citrix Gateway 13.0, versiones anteriores a 13.0-88.12.
- Citrix ADC and Citrix Gateway 12.1, versiones anteriores a 12.1.65.21.
- Citrix ADC 12.1-FIPS, versiones anteriores a 12.1-55.289.
- Citrix ADC 12.1-NDcPP, versiones anteriores a 12.1-55.289.

Descripción:

Se ha reportado un nuevo aviso de seguridad sobre tres vulnerabilidades que afectan a Citrix Gateway y Citrix ADC, que permitirían a un atacante realizar omisión de autenticación, obtener acceso no autorizado y tomar el control del sistema afectado.

- CVE-2022-27510, de severidad “Crítica”, con una puntuación asignada de 9.8. Esta vulnerabilidad se debe a una falla en el control de configuraciones VPN del dispositivo. Esto permitiría a un atacante realizar omisión de autenticación cuando el dispositivo se utiliza como puerta de enlace (dispositivos que utilizan la funcionalidad *SSL VPN* o se utilizan como proxy *ICA* con autenticación habilitada).

- CVE-2022-27513, de severidad “Crítica”, con una puntuación asignada de 9.6. Esta vulnerabilidad se debe a una falla en el control de autenticación de datos. Esto permitiría a un atacante obtener acceso no autorizado al sistema solo si el dispositivo está configurado como puerta de enlace (*SSL VPN*) y la funcionalidad de proxy *RDP* está habilitada.

- CVE-2022-27516, de severidad “Crítica”, con una puntuación asignada de 9.8. Esta vulnerabilidad se debe a una falla en la protección de fuerza bruta de inicio de sesión. Esto permitiría a un atacante tomar el control del sistema afectado solo si el dispositivo está configurado como puerta de enlace (*SSL VPN*) o servidor virtual *AAA* con la configuración "*Max Login Attempts*".

Impacto:

La explotación exitosa de estas vulnerabilidades permitiría a un atacante realizar omisión de autenticación, obtener acceso no autorizado y tomar el control del sistema afectado.

Solución:

Recomendamos instalar las actualizaciones correspondientes provistas por el fabricante en el siguiente enlace:

- https://www.citrix.com/support/

Información adicional:

- https://www.bleepingcomputer.com/news/security/citrix-urges-admins-to-patch-critical-adc-gateway-auth-bypass/
- https://support.citrix.com/article/CTX463706/citrix-gateway-and-citrix-adc-security-bulletin-for-cve202227510-cve202227513-and-cve202227516
- Citrix ADC and Citrix Gateway are affected by a critical auth bypassSecurity Affairs
- Patch ASAP: Critical Citrix, VMware Bugs Threaten Remote Workspaces With Takeover (darkreading.com)
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-27510
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-27513
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-27516
- https://www.citrix.com/support/