Citrix ha publicado actualizaciones de seguridad para corregir dos vulnerabilidades en NetScaler ADC y NetScaler Gateway, entre ellas una falla crítica que podría ser utilizada para filtrar información sensible de la aplicación.

Las vulnerabilidades se detallan a continuación:

- CVE-2026-3055 (puntuación CVSS: 9.3) – Validación insuficiente de entradas que provoca una lectura de memoria fuera de límites
- CVE-2026-4368 (puntuación CVSS: 7.7) – Condición de carrera que puede ocasionar mezcla de sesiones de usuario

La empresa de ciberseguridad Rapid7 explicó que CVE-2026-3055 corresponde a una lectura fuera de límites que podría ser explotada por atacantes remotos no autenticados para extraer información potencialmente sensible desde la memoria del dispositivo.

No obstante, para que el ataque tenga éxito, el dispositivo Citrix ADC o Citrix Gateway debe estar configurado como proveedor de identidad SAML (SAML IdP), lo que implica que las configuraciones predeterminadas no se ven afectadas. Para verificar si el equipo ha sido configurado como perfil SAML IdP, Citrix recomienda a los clientes revisar la configuración de NetScaler en busca de la cadena específica: «*add authentication samlIdPProfile .«**

Por otro lado, CVE-2026-4368 requiere que el dispositivo esté configurado como gateway (por ejemplo, SSL VPN, ICA Proxy, CVPN o RDP Proxy) o como servidor de Autenticación, Autorización y Contabilidad (AAA). Los usuarios pueden comprobar la configuración de NetScaler para confirmar si sus dispositivos están configurados como alguno de estos nodos:

- Servidor virtual AAA – *add authentication vserver .*
- Gateway – *add vpn vserver .*

Las vulnerabilidades afectan a las versiones de NetScaler ADC y NetScaler Gateway 14.1 anteriores a 14.1-66.59 y 13.1 anteriores a 13.1-62.23, así como a NetScaler ADC 13.1-FIPS y 13.1-NDcPP anteriores a 13.1-37.262. Se recomienda a los usuarios aplicar las

actualizaciones más recientes lo antes posible para garantizar una protección adecuada.

Aunque no hay evidencia de que estas fallas hayan sido explotadas activamente, las vulnerabilidades en dispositivos NetScaler han sido utilizadas repetidamente por actores maliciosos (CVE-2023-4966, conocida como Citrix Bleed, CVE-2025-5777 o Citrix Bleed 2, CVE-2025-6543 y CVE-2025-7775), lo que hace fundamental que los usuarios actualicen sus sistemas.

*«CVE-2026-3055 permite a atacantes no autenticados filtrar y leer memoria sensible de implementaciones NetScaler ADC. Si suena familiar, es porque lo es: esta vulnerabilidad recuerda sospechosamente a Citrix Bleed y Citrix Bleed 2, que siguen siendo eventos críticos para muchos,»* declaró Benjamin Harris, CEO y fundador de watchTowr, a The Hacker News.

*«Los dispositivos NetScaler son soluciones críticas que han sido constantemente objetivo para obtener acceso inicial a entornos empresariales. Aunque el aviso acaba de publicarse, los defensores deben actuar con rapidez. Cualquier organización que utilice versiones afectadas necesita aplicar parches de inmediato. La explotación es muy probable en el corto plazo.»*