Durante las últimas semanas, Citrix ha estado implementado en privado una actualización crítica de software para sus clientes empresariales, que parchea múltiples vulnerabilidades de seguridad que afectan la plataforma de colaboración de contenido Citrix ShareFile.

Dimitri van de Giessen, un hacker ético, informó antes de la publicación, que Citrix trabajaba en un aviso de seguridad que ahora está disponible en el sitio web de la compañía.

Citrix ShareFile es una solución de intercambio de archivos de nivel empresarial para compañías que utilizan los empleados para intercambiar de forma segura datos comerciales confidenciales y de propiedad exclusiva.

El software ofrece un entorno de nube local y seguro para el almacenamiento de datos con capacidades de auditoría y controles de cumplimiento normativo. Por ejemplo, una empresa puede bloquear o borrar remotamente datos de dispositivos móviles portencialmente comprometidos, o cuando se pierden o son robados.

Los problemas de seguridad recientemente identificados (CTX-CVE-2020-7473), afectan específicamente a los controladores de zona de almacenamiento Citrix ShareFile locales administrados por el cliente, un componente que almacena datos corporativos detrás del firewall.

Las vulnerabilidades en cuestión son:

- CVE-2020-7473
- CVE-2020-8982
- CVE-2020-8983

Según el aviso, en caso de que estas vulnerabilidades sean explotadas, podrían permitir que un hacker no autenticado comprometa potencialmente el controlador de zonas de almacenamiento y acceda a documentos y carpetas sensibles de ShareFile.

Versiones de Citrix ShareFile afectadas y parcheadas

Las versiones de ShareFile locales afectadas son: 5.9.0 / 5.8.0 / 5.7.0/ 5.5.0 y anteriores, por lo que se recomienda actualizar inmediatamente al controlador de zonas de almacenamiento 5.10.0 / 5.9.1 / 5.8.1 o posterior.

Se debe tomar en cuenta que si la zona de almacenamiento se creó en cualquiera de las versiones afectadas, simplemente actualizar el software a una versión parcheada no resolverá completamente el problema.

Para una solución adecuada, la compañía lanzó por separado una herramienta de mitigación que se debe ejecutar primero en el controlador de zonas de almacenamiento primario y luego en cualquier controlador secundario.

> *«Una vez que la herramienta se ejecute con éxito en su zona principal, NO DEBE revertir ningún cambio. Revertir los cambios hará que su zona no esté disponible»*, advierte el aviso.

Además de la solución local, las versiones en la nube de los controladores de zona de almacenamiento ShareFile también se vieron afectadas, pero la compañía ya las parchó y no requiere ninguna acción adicional por parte de los usuarios.

Hasta el momento, no existen muchos detalles técnicos sobre las vulnerabilidades, pero una inspección de parche inicial realizada por Dimitri, reveló que al menos uno de los defectos reside en un antiguo kit de herramientas ASP.NET que Citrix ShareFile utilizaba.

La versión obsoleta de 9 años de AjaxControlToolkit que supuestamente se incluye con las versiones afectadas del software ShareFile, contiene vulnerabilidades de ejecución remota de código y recorrido de directorio (CVE-2015-4670), que se divulgaron públicamente en 2015.

Para verificar si la implementación de Citrix ShareFile se ve afectada o no, se puede visitar la siguiente URL en el navegador web, y si la página se pone en blanco, es vulnerable, si muestra un error 404, no está defectuosa o ha sido reparada.

> https://yoursharefileserver.companyname.com/UploadTest.aspx

Según Dimitri, la herramienta de mitigación realiza algunos cambios en el archivo web.config y luego elimina UploadTest.aspx y XMLFeed.aspx de los servidores afectados.