Alerta de seguridad cibernética	9VSA20-00286-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	18 de agosto de 2020
Última revisión	18 de agosto de 2020

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, comparte la información obtenida de Citrix respecto a cinco vulnerabilidades -2 de ellas críticas- que afectan Citrix Endpoint Managment para móviles (CEM Movile Server). El presente informe incluye la respectiva medida de mitigación.

Vulnerabilidades

CVE-2020-8208
CVE-2020-8209
CVE-2020-8210
CVE-2020-8211
CVE-2020-8212

Impactos

Dos vulnerabilidades críticas (CVE-2020-8208 y CVE-2020-8209) y tres vulnerabilidades medianas y bajas (CVE-2020-8210, CVE-2020-8211 y CVE-2020-8212) han sido descubiertas en XenMobile Server. No se han entregado mayores detalles técnicos respecto a las vulnerabilidades, pero revelaron que ya se comunicaron con los CERTs y sus clientes, y que el 70% de ellos ya han aplicado las medidas de seguridad.
Es necesario aplicar los parches urgentemente, ya que si bien, no se conocen exploits que aprovechen estas vulnerabilidades, Citrix prevé que atacantes rápidamente desarrollarán formas de realizar ataques.
Fuentes externas indican que de no subsanar las vulnerabilidades, un atacante podría obtener datos sensibles como archivos de configuración y llaves de encriptación. Además, si el atacante logra obtener credenciales de dominio para LDAP, el ataque podría extenderse fuera de la red, permitiendo comprometer datos de recursos externos.

Productos Afectados

Las siguientes versiones de Citrix Endpoint Managment (CEM) son afectados por vulnerabilidades nivel crítico:
XenMobile Server 10.12 previo RP2
XenMobile Server 10.11 previo RP4
XenMobile Server 10.10 previo RP6
XenMobile Server previo 10.9 RP5

Las siguientes versiones de Citrix Endpoint Managment (CEM) son afectados por vulnerabilidades nivel medio y bajo:
XenMobile Server 10.12 previo RP3
XenMobile Server 10.11 previo RP6
XenMobile Server 10.10 previo RP6
XenMobile Server previo 10.9 RP5

Clientes que utilicen la versión Cloud de CEM no requieren tomar medidas de mitigación.

Mitigaciones

Aplicar los parches de seguridad requeridos por la versión utilizada.
XenMobile Server 10.12 RP3: https://support.citrix.com/article/CTX277473
XenMobile Server 10.11 RP6: https://support.citrix.com/article/CTX277698
XenMobile Server 10.10 RP6: https://support.citrix.com/article/CTX279101
XenMobile Server 10.9 RP5: https://support.citrix.com/article/CTX279098

Enlaces

https://support.citrix.com/article/CTX277457
https://www.citrix.com/blogs/2020/08/11/citrix-provides-security-update-on-citrix-endpoint-management/
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-8208
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-8209
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-8210
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-8211
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-8212