Alerta de seguridad cibernética	9VSA21-00369-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	21 de enero de 2021
Última revisión	21 de enero de 2021

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 entregada por TerraMaster, sobre vulnerabilidades que afectan a TerraMaster TOS.

Este informe incluye las medidas de mitigación, consistentes en instalar las últimas actualizaciones de los productos afectados.

Vulnerabilidades

CVE-2020-28184
CVE-2020-28185
CVE-2020-28186
CVE-2020-28187
CVE-2020-28188
CVE-2020-28189
CVE-2020-28190

Impacto

CVE-2020-28184: Esta vulnerabilidad permite a un atacante remoto realizar un ataque XSS. Existe debido a una sanitización insuficiente de los datos entregados por el usuario y que pasan por el parámetro “mod” en “/module/index[.]php”. Un atacante remoto autenticado puede engañar a la víctima para que ingrese a un enlace especialmente diseñado y ejecute HTML y código script arbitrario.

CVE-2020-28185: Esta vulnerabilidad permite a un atacante remoto ganar acceso a información potencialmente sensible. La vulnerabilidad existe debido a una inyección de email en el parámetro “username” en “wizard/initialise[.]php”. Un atacante remoto puede identificar usuarios validos dentro del sistema.

CVE-2020-28186: Esta vulnerabilidad afecta la función de Recordatorio de Contraseña, que es susceptible a una inyección de email, permitiendo a un atacante recibir el código de verificación. El ataque solo funciona si el usuario especificó un “email de seguridad” en la cuenta.

CVE-2020-28187: Esta vulnerabilidad permite a un atacante remoto autenticado realizar ataques de tipo “directory traversal”, debido a un error de validación de entradas. El atacante puede enviar una solicitud HTTP especialmente diseñada y leer, editar o eliminar cualquier archivo dentro del sistema de archivos.

CVE-2020-28188: Esta vulnerabilidad permite a un atacante remoto no autenticado inyectar comandos OS en el sistema objetivo. La vulnerabilidad existe debido a una validación inadecuada de entradas en el parámetro “Event” en “/include/makecvs[.]php”

CVE-2020-28189: Esta vulnerabilidad permite a un atacante remoto ganar acceso no autorizado a funciones restringidas, y existe a causa de restricciones de acceso inapropiadas. Un atacante autenticado remoto puede evadir las restricciones de “solo lectura” y obtener acceso total a cualquier carpeta dentro del NAS.

CVE-2020-28190: Esta vulnerabilidad permite a un atacante remoto realizar un ataque de hombre en el medio por culpa de que las aplicaciones y actualizaciones de software son entregadas y chequeadas a través de un canal de comunicación no encriptado (HTTP).

Productos afectados
TerraMaster TOS 4.2.06.

Mitigación
Instalar las actualizaciones desde el sitio del proveedor.

Enlaces
https://www.ihteam.net/advisory/terramaster-tos-multiple-vulnerabilities/

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-28184

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-28185

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-28186

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-28187

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-28188

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-28189

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-28190

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2021.01.21 11:10:05 -03'00'