ACTUALIZACIÓN - EXPLOTACIÓN DE VULNERABILIDADES DE APACHE SERVER (06/14/OCTUBRE/2021)

Luego de haberse emitido la publicación de la prioridad de riesgo CVE-2021-41773 que afecta a la aplicación Apache Server, se ha identificado que la actualización de corrección contenida en la actualización 2.4.50 es insuficiente ante la configuración especializada de ataques de tipo path traversal y por tanto se ha emitido la actualización 2.4.51. Adicionalmente se ha toma conocimiento de la explotación de ataques al mod_proxy que fueron identificadas en el reporte de prioridad de riesgo CVE-2021-40438.

Los desarrolladores de apache server han emitido parches para corregir vulnerabilidades de seguridad que estarían siendo activamente escaneadas y explotadas por ciber atacantes. Apache es un servidor HTTP de código abierto que por sus servicios HTTP, se ha convertido en el servidor web más popular en sistemas de información tanto UNIX como Windows. Un error en el proceso de normalización de identificador de recursos uniforme URI permitiría la ejecución de ataques de tipo path traversal e inyección de código por URL, y así acceder sin autorización a activos de información, incluso siendo posible ejecutar ataques de denegación de servicio. Las vulnerabilidades detectadas y que estarían siendo explotadas afectan a la versión 2.4.49.

En consideración al alto riesgo contra la confidencialidad, integridad y disponibilidad de los activos de información administrados y gestionados por la herramienta APACHE HTTP SERVER, el EcuCERT recomienda a su comunidad objetivo, tomar en consideración las siguientes recomendaciones:

1. De manera urgente actualizar la herramienta a la versión 2.4.51.

2. Establecer restricciones en los archivos de configuración apache2.conf

3. Actualizar las credenciales de los perfiles de administración y usuarios gestionados en la herramienta.

4. Implementar un WAF (Firewall de aplicaciones) para proteger el acceso a sitios web.

Referencias

APACHE HTTP SERVER PROJECT. (2021). Apache HTTP server 2.4 vulnerabilities. Disponible en https://httpd.apache.org/security/vulnerabilities_24.html

CVE. (2021). CVE-2021-42013. Disponible en https://nvd.nist.gov/vuln/detail/CVE-2021- 42013

CVE. (2021). CVE-2021-41773. Disponible en https://nvd.nist.gov/vuln/detail/CVE-2021- 41773

CVE. (2021). CVE-2021-41524. Disponible en https://nvd.nist.gov/vuln/detail/CVE-2021- 41524

CVE. (2021). CVE-2021-40438. Disponible en https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-40438