BOLETÍN DE ALERTA

Boletín Nro.: 2022-14

Fecha de publicación: 03/03/2022

Tema: Múltiples vulnerabilidades en productos de Fortinet.

Softwares afectados:

- FortiMail versiones anteriores a 7.0.1.
- FortiPortal versiones anteriores a 6.0.6.
- FortiWLM versiones anteriores a 8.6.3.
- FortiManager versiones anteriores a 7.0.2.
- FortiAnalyzer versiones anteriores a 7.0.2.
- Forti OS versiones anteriores a 6.4.3.
- FortiToken Mobile (Android) versiones anteriores a 5.2.0.
- FortiAP-C 5.4.0 hasta la 5.4.3

Descripción:

Fortinet ha publicado múltiples avisos de seguridad que contemplan 11 (once) vulnerabilidades, de las cuales 1 (una) es Crítica, 5 (cinco) de criticidad alta, 1 (una) de criticidad media y 4 (cuatro) de criticidad baja. Estas vulnerabilidades permitirían a un atacante realizar ejecución remota de código (RCE), inyección de comandos SQL, evasión de controles de seguridad y acceder a información sensible. Se destacan las siguientes vulnerabilidades:

- CVE-2021-36166 de severidad crítica, con una puntuación de 9.8. Esta vulnerabilidad se debe a una falla en el proceso de autenticación de FortiMail, que permite a través de la observación de ciertas propiedades del sistema adivinar el token de autenticación de una cuenta de administración. Un atacante remoto podría aprovechar esta situación para obtener acceso completo al sistema afectado con dicho token. Los softwares afectados FortiMail en sus versiones anteriores a 7.0.1.

- CVE-2021-32586 de severidad alta, con una puntuación de 7.7. Esta vulnerabilidad se debe a una validación incorrecta de un *input* de la CGI del servidor web de FortiMail. Un atacante no autenticado podría enviar peticiones HTTP especialmente diseñadas para alterar el entorno del intérprete de scripts del sistema y así comprometer el sistema afectado. Los softwares afectados son FortiMail en sus versiones anteriores a 7.0.1

- CVE-2021-43077 de severidad Alta, con una puntuación de 8.8. Esta vulnerabilidad se debe a un error en el componente *AP Monitor Handler*, que no valida correctamente

la entrada de datos que realiza el usuario. Un atacante podría enviar una petición maliciosa con el objetivo de ejecutar código SQL arbitrario. Los softwares afectados son FortiWLM en sus versiones anteriores a 8.6.3.

Se puede acceder al listado completo de las vulnerabilidades subsanadas aquí.

Impacto:

La explotación de estas vulnerabilidades permitiría a un atacante realizar ejecución remota de código, inyección de comandos SQL, evasión de controles de seguridad y acceder a información sensible en el dispositivo afectado.

Detección:

Verificar si se posee instalado los softwares y sus versiones respectivamente vulnerables en el equipo.

- FortiMail versiones anteriores a 7.0.1.
- FortiPortal versiones anteriores a 6.0.6.
- FortiWLM versiones anteriores a 8.6.3.
- FortiManager versiones anteriores a 7.0.2.
- FortiAnalyzer versiones anteriores a 7.0.2.
- Forti OS versiones anteriores a 6.4.3.
- FortiToken Mobile (Android) versiones anteriores a 5.2.0.
- FortiAP-C 5.4.0 hasta 5.4.3

Solución:

Se recomienda instalar las actualizaciones más recientes utilizando de referencias las siguientes guías provistas por el fabricante.

- FortiMail: https://docs.fortinet.com/document/fortimail/6.4.2/administration-guide/107638/installing-firmware
- FortiPortal: https://docs.fortinet.com/document/fortiportal/5.3.4/administration-guide/326757/upgrading-fortiportal-software
- FortiWLM: https://docs.fortinet.com/document/fortiwlm/8.5.3/fortiwlm-release-notes/991062/upgrade-procedure
- FortiManager: https://docs2.fortinet.com/document/fortimanager/6.0.0/upgrade-guide/319480/upgrading-fortimanager-firmware
- FortiAnalyzer: https://docs.fortinet.com/document/fortianalyzer/7.0.2/upgrade-guide/262607/upgrading-fortianalyzer-firmware

- FortiOS: https://docs.fortinet.com/document/fortigate/6.2.10/cookbook/596131/upgrading-the-firmware
- FortiToken Mobile: https://play.google.com/store/apps/details?id=com.fortinet.android.ftm&hl=en&gl=US
- FortiAP-C: https://docs.fortinet.com/document/fortiap/5.4.3/fortiap-c-release-notes/425688/introduction

Información adicional:

- https://portal.cci-entel.cl/Threat_Intelligence/Boletines/1163/
- https://nvd.nist.gov/vuln/detail/CVE-2021-36166
- https://nvd.nist.gov/vuln/detail/CVE-2021-32586
- https://nvd.nist.gov/vuln/detail/CVE-2021-43077