BOLETÍN DE ALERTA

Boletín Nro.: 2021-13

Fecha de publicación: 25/05/2021

Tema: Vulnerabilidades críticas que afectan al software de monitoreo de TI de Nagios.

Sistemas afectados:

- Nagios XI versiones anteriores a 5.8.0.
- Nagios Fusion versiones anteriores a 4.1.8.

Descripción:

Los investigadores de ciberseguridad de Skylight Cyber han revelado detalles sobre 13 vulnerabilidades en las aplicaciones de monitoreo de red de Nagios.

Entre ellos, la más grave rastreada como CVE-2020-28648 (puntaje CVSS: 8.8), este es el componente de autodescubrimiento Nagios XI, que los investigadores usaron como punto de partida para desencadenar una cadena de exploits que conecta un total de cinco vulnerabilidades para lograr un ataque de compromiso total. Es decir, si un atacante compromete el sitio de un cliente monitoreado usando el servidor Nagios XI, podría comprometer el servidor de administración del operador y todos los demás clientes monitoreados.

Los expertos informaron sus hallazgos a Nagios en octubre de 2020. En noviembre de 2020, la compañía lanzó actualizaciones para solucionar los problemas.

A continuación, se incluye un resumen de las 13 vulnerabilidades:

- CVE-2020-28648 - Ejecución remota de código autenticado por Nagios XI (desde el contexto de un usuario con pocos privilegios).
- CVE-2020-28900 - Escalada de privilegios de Nagios Fusion y XI de nagios a root a través de upgrade_to_latest.sh.
- CVE-2020-28901 - Escalada de privilegios de Nagios Fusion de apache a Nagios mediante la inyección de comandos en el parámetro component_dir en cmd_subsys.php.

- CVE-2020-28902 - Escalada de privilegios de Nagios Fusion de apache a nagios mediante la inyección de comandos en el parámetro de zona horaria en cmd_subsys.php.
- CVE-2020-28903 - XSS en Nagios XI cuando un atacante tiene control sobre un servidor fusionado.
- CVE-2020-28904 - Escalada de privilegios de Nagios Fusion de apache a nagios mediante la instalación de componentes maliciosos.
- CVE-2020-28905 - Ejecución remota de código autenticado por Nagios Fusion (desde el contexto de usuario con privilegios bajos).
- CVE-2020-28906 - Escalada de privilegios de Nagios Fusion y XI de nagios a root mediante la modificación de fusion-sys.cfg / xi-sys.cfg.
- CVE-2020-28907 - Escalada de privilegios de Nagios Fusion de apache a root a través de upgrade_to_latest.sh y modificación de la configuración del proxy.
- CVE-2020-28908 - Escalada de privilegios de Nagios Fusion de apache a nagios mediante inyección de comandos (causada por una desinfección deficiente) en cmd_subsys.php.
- CVE-2020-28909 - Escalada de privilegios de Nagios Fusion de nagios a root mediante la modificación de scripts que se pueden ejecutar como sudo.
- CVE-2020-28910 - Escalada de privilegios getprofile.sh de Nagios XI.
- CVE-2020-28911 - Divulgación de información de Nagios Fusion: el usuario con menos privilegios puede autenticarse en el Servidor Fusion cuando se almacenan las credenciales.

La explotación exitosa de las vulnerabilidades, de manera combinada, podría permitir a los atacantes activar secuencias de comandos entre sitios y ejecutar código JavaScript en el contexto de los usuarios de Fusion para controlar el servidor Fusion, tomar el control e irrumpir en servidores XI ubicados en otros sitios de clientes.

Los investigadores de Eastern Alliance también lanzaron una herramienta de post-explotación basada en PHP llamada SoyGun, que vincula las vulnerabilidades y "permite a los atacantes usar las credenciales de usuario de Nagios XI y el acceso HTTP al servidor Nagios XI para controlar completamente la implementación de Nagios Fusion".

Impacto:

La explotación exitosa de algunas combinaciones de vulnerabilidades permite a un atacante remoto el control completo de los servidores Nagios XI ubicados en otros sitios de clientes.

Solución:

- Actualice a la última versión de Nagios XI 5.8.3 y Nagios Fusion 4.1.9.

Información adicional:

- https://www.nagios.com/products/security/
- https://www.jioforme.com/details-disclosed-about-critical-flaws-affecting-nagios-it-monitoring-software/454235/
- https://thehackernews.com/2021/05/details-disclosed-on-critical-flaws.html