BOLETÍN DE ALERTA

Boletín Nro.: 2021-26

Fecha de publicación: 24/09/2021

Tema: Vulnerabilidades críticas en productos Nagios.

.

Productos afectados:

- Nagios XI, anteriores a la versión 5.8.5;
- Nagios XI Docker Wizard, anteriores a la versión 1.1.3;
- Nagios XI WatchGuard Wizard, anteriores a la versión 1.4.8;
- Nagios XI Switch Wizard, anteriores a la versión 2.5.7.

Descripción:

Se han descubierto 11 vulnerabilidades de seguridad en los sistemas de administración de red de Nagios. Nagios es un sistema de monitoreo de código abierto para sistemas informáticos.

Las vulnerabilidades tienen los siguientes identificadores:

- CVE-2021-37344, de severidad crítica con una puntuación de 9.8, debido a esta vulnerabilidad el asistente de conmutación de Nagios XI versiones anteriores a la 2.5.7 son vulnerables a la ejecución remota de código a través de la neutralización inadecuada de elementos especiales utilizados en un comando del sistema operativo (inyección de comando del sistema operativo).
- CVE-2021-37346, de severidad crítica con una puntuación de 9.8, debido a esta vulnerabilidad las versiones de Nagios XI WatchGuard Wizard anteriores a la 1.4.8 son vulnerables a la ejecución remota de código a través de la neutralización inadecuada de elementos especiales utilizados en un comando del sistema operativo (inyección de comando del sistema operativo).

- CVE-2021-37350, de severidad crítica con una puntuación de 9.8, debido a esta vulnerabilidad las versiones de Nagios XI anteriores a la 5.8.8, son vulnerables a una inyección SQL en Bulk Modifications Tool. debido a una incorrecta desinfección de entrada.
- CVE-2021-37353, de severidad crítica con una puntuación de 9.8, debido a esta vulnerabilidad las versiones de Nagios XI Docker Wizard anteriores a la 1.1.3, son vulnerables a una falsificación de solicitudes del lado del servidor (SSRF) debido a una desinfección incorrecta en table_population.php.
- CVE-2021-37343, de severidad alta con una puntuación de 8.8, existe una vulnerabilidad de recorrido de ruta en Nagios XI por debajo del componente de AutoDiscovery de la versión 5.8.5 y podría conducir a un RCE post-autenticado en el contexto de seguridad del usuario que ejecuta Nagios.
- CVE-2021-37345, de severidad alta con una puntuación de 7.8, las versiones de Nagios XI anteriores a la versión 5.8.5 son vulnerables a la escalada de privilegios local debido a que xi-sys.cfg se está importando desde el directorio var para algunos scripts con permisos elevados.
- CVE-2021-37347, de severidad alta con una puntuación de 7.8, las versiones de Nagios XI anteriores a la versión 5.8.5 son vulnerables a la escalada de privilegios local porque getprofile.sh no valida el nombre de directorio que recibe como argumento.
- CVE-2021-37349, de severidad alta con una puntuación de 7.8, las versiones de Nagios XI anteriores a la versión 5.8.5 son vulnerables a la escalada de privilegios local porque cleaner.php no desinfecta la entrada leída de la base de datos.
- CVE-2021-37348, de severidad alta con una puntuación de 7.8, las versiones de Nagios XI anteriores a la versión 5.8.5, son vulnerables a la inclusión de archivos locales a través de una limitación incorrecta de un nombre de ruta en index.php.

- CVE-2021-37352, de severidad media con una puntuación de 6.1, existe una vulnerabilidad de redireccionamiento abierto en las versiones de Nagios XI anteriores a la 5.8.5 que podría provocar suplantación de identidad. Para aprovechar la vulnerabilidad, un atacante podría enviar un enlace que tenga una URL especialmente diseñada y convencer al usuario de que haga clic en el enlace.
- CVE-2021-37351, de severidad media con una puntuación de 5.3, las versiones de Nagios XI Docker Wizard anteriores a la versión 1.1.3 son vulnerables a una falsificación de solicitudes del lado del servidor (SSRF) debido a una desinfección incorrecta en table_population.php.

Impacto:

La explotación exitosa de las vulnerabilidades podría permitir a un atacante remoto ejecutar código remoto (RCE) y obtener el control total del sistema.

Solución:

Nagios abordó las vulnerabilidades a través de actualizaciones de sus productos Nagios XI, Nagios XI Docker Wizard, Nagios XI WatchGuard Wizard y Nagios XI Switch Wizard. Se recomienda encarecidamente actualizar de forma inmediata los sistemas afectados.

Información adicional:

- https://thehackernews.com/2021/09/new-nagios-software-bugs-could-let.html
- https://www.nagios.com/products/security/