OPMANAGER:

Subject line:
[CRITICO] OpManager - Aviso de seguridad sobre CVE-2020-11946

Hola,

Saludos desde ManageEngine OpManager. Este es un correo de aviso de seguridad que trata una **vulnerabilidad en la llamada sin autenticación al servlet** corregida en la última versión de OpManager v12.4.196. SE RECOMIENDA ALTAMENTE que lea este correo para verificar si su instalación se ha visto afectada o no, y si está afectada, aprender a resolverla.

Nombre del problema y descripción:

Revelación de clave API no autenticada - Hubo un método de acceso no autenticado para obtener la clave API que se descubrió en el producto. El autor podría explotar esto para agregar un usuario administrador mediante una llamada a la API y realizar operaciones a nivel de administrador. Esta es una vulnerabilidad de seguridad **crítica**. (Consulte: CVE-2020-11946)

¿Quién ha sido afectado por esta vulnerabilidad?

Cualquier instalación de OpManager con número de compilación entre **12.3.xxx y 12.4.195** (para OpManager v12.3 y v12.4), y número de compilación entre **12.5.001 y 12.5.119** (para OpManager v12.5) podría explotarse utilizando esta vulnerabilidad .

Si no está seguro en qué compilación se encuentra, puede encontrarlo fácilmente siguiendo estos pasos:

1. En el cliente web, haga clic en el icono Perfil en la esquina superior derecha de la pantalla.
2. En la pestaña "Acerca de", puede encontrar la versión en el campo "Número de compilación".

¿Cómo resolvió el equipo de seguridad de ManageEngine esta vulnerabilidad?

@kuncho, un investigador de seguridad independiente, nos informó este problema el 12

de abril. Tan pronto como nos informaron de esto, se agregaron medidas de autenticación adecuadas para la llamada API y la última versión del producto con la solución, es decir, **OpManager v12.4.196** fue liberada el 22 de abril de 2020.

¿Cómo puedo identificar si mi instalación se ha visto comprometida?

1. Compruebe si hay nuevas cuentas de usuario de OpManager que parezcan sospechosas, navegando a **Configuración> Configuración general> Administración de usuarios**. Si hay alguna, verifique que no haya sido creado por otros usuarios administradores (si corresponde) y elimine ese nuevo perfil de usuario de inmediato.
2. Además, puede verificar los logs de acceso para cualquier solicitud sendData no autenticada. En la carpeta "logs" en el directorio de instalación, abra **access_log.txt** y verifique si se ha realizado alguna de las siguientes llamadas API desde cualquier IP externa, es decir, sin el sufijo "- localhost" al lado de la dirección:
    i. sendData - se utiliza para exponer la clave de API al atacante.
    ii. addUser - posible acción de agregar usuario realizada utilizando la clave obtenida
    iii. testNProfile - posible RCE realizado en algunos / todos los dispositivos en la red

Si nota alguno de estos en su configuración, CIERRE INMEDIATAMENTE LA INSTALACIÓN y contacte a nuestro equipo de soporte.

¿Qué puedo hacer para corregir esta vulnerabilidad?

Si está en cualquier compilación de OpManager hasta la 12.4.195, se recomienda actualizar a OpManager v12.4.196 directamente desde nuestra página de service packs. Para los usuarios de OpManager versión 12.5, se recomienda actualizar a la compilación 12.5.120.

Alternativamente, también puede comunicarse directamente con nuestro equipo de seguridad para obtener ayuda con la actualización en itom-upgrades@manageengine.com o enviar una solicitud de soporte desde nuestra página de soporte para obtener asistencia de nuestros técnicos.

NCM:

Subject line:
[CRITICO] Network Configuration Manager - Aviso de seguridad sobre CVE-2020-11946

Hola,

Saludos desde ManageEngine Network Configuration Manager. Este es un correo de aviso de seguridad que trata una **vulnerabilidad en la llamada sin autenticación al servlet** corregida en la última versión de Network Configuration Manager v12.4.196. SE RECOMIENDA ALTAMENTE que lea este correo para verificar si su instalación se ha visto afectada o no, y si está afectada, aprender a resolverla.

Nombre del problema y descripción:

Revelación de clave API no autenticada - Hubo un método de acceso no autenticado para obtener la clave API que se descubrió en el producto. El autor podría explotar esto para agregar un usuario administrador mediante una llamada a la API y realizar operaciones a nivel de administrador. Esta es una vulnerabilidad de seguridad **crítica**. (Consulte: CVE-2020-11946)

¿Quién ha sido afectado por esta vulnerabilidad?

Cualquier instalación de Network Configuration Manager con número de compilación entre **12.3.xxx y 12.4.195** (para NCM v12.3 y v12.4), y número de compilación entre **12.5.001 y 12.5.119** (para NCM v12.5) podría explotarse utilizando esta vulnerabilidad .

Si no está seguro en qué compilación se encuentra, puede encontrarlo fácilmente siguiendo estos pasos:

1. En el cliente web, haga clic en el icono Perfil en la esquina superior derecha de la pantalla.
2. En la pestaña "Acerca de", puede encontrar la versión en el campo "Número de compilación".

¿Cómo resolvió el equipo de seguridad de ManageEngine esta vulnerabilidad?

@kuncho, un investigador de seguridad independiente, nos informó este problema el 12 de abril. Tan pronto como nos informaron de esto, se agregaron medidas de autenticación adecuadas para la llamada API y la última versión del producto con la solución, es decir, **Network Configuration Manager v12.4.196** fue liberada el 22 de abril de 2020.

¿Cómo puedo identificar si mi instalación se ha visto comprometida?

1. Compruebe si hay nuevas cuentas de usuario de NCM que parezcan sospechosas, navegando a **Configuración> Configuración general> Administración de usuarios**. Si hay alguna, verifique que no haya sido creado por otros usuarios administradores (si corresponde) y elimine ese nuevo perfil de usuario de inmediato.
2. Además, puede verificar los logs de acceso para cualquier solicitud sendData no autenticada. En la carpeta "logs" en el directorio de instalación, abra **access_log.txt** y verifique si se ha realizado alguna de las siguientes llamadas API desde cualquier IP externa, es decir, sin el sufijo "- localhost" al lado de la dirección:
    i. sendData - se utiliza para exponer la clave de API al atacante.
    ii. addUser - posible acción de agregar usuario realizada utilizando la clave obtenida
    iii. testNProfile - posible RCE realizado en algunos / todos los dispositivos en la red

Si nota alguno de estos en su configuración, CIERRE INMEDIATAMENTE LA INSTALACIÓN y contacte a nuestro equipo de soporte.

¿Qué puedo hacer para corregir esta vulnerabilidad?

Si está en cualquier compilación de NCM hasta la 12.4.195, se recomienda actualizar a Network Configuration Manager v12.4.196 directamente desde nuestra página de service packs. Para los usuarios de NCM versión 12.5, se recomienda actualizar a la compilación 12.5.120.

Alternativamente, también puede comunicarse directamente con nuestro equipo de

seguridad para obtener ayuda con la actualización en itom-upgrades@manageengine.com o enviar una solicitud de soporte desde nuestra página de soporte para obtener asistencia de nuestros técnicos.

NETFLOW ANALYZER:

Subject line:
[CRITICO] NetFlow Analyzer - Aviso de seguridad sobre CVE-2020-11946

Hola,

Saludos desde ManageEngine NetFlow Analyzer. Este es un correo de aviso de seguridad que trata una **vulnerabilidad en la llamada sin autenticación al servlet** corregida en la última versión de NetFlow Analyzer v12.4.196. SE RECOMIENDA ALTAMENTE que lea este correo para verificar si su instalación se ha visto afectada o no, y si está afectada, aprender a resolverla.

Nombre del problema y descripción:

Revelación de clave API no autenticada - Hubo un método de acceso no autenticado para obtener la clave API que se descubrió en el producto. El autor podría explotar esto para agregar un usuario administrador mediante una llamada a la API y realizar operaciones a nivel de administrador. Esta es una vulnerabilidad de seguridad **crítica**. (Consulte: CVE-2020-11946)

¿Quién ha sido afectado por esta vulnerabilidad?

Cualquier instalación de NetFlow Analyzer con número de compilación entre **12.3.xxx y 12.4.195** (para NFA v12.3 y v12.4), y número de compilación entre **12.5.001 y 12.5.119** (para NFA v12.5) podría explotarse utilizando esta vulnerabilidad .

Si no está seguro en qué compilación se encuentra, puede encontrarlo fácilmente siguiendo estos pasos:

1. En el cliente web, haga clic en el icono Perfil en la esquina superior derecha de la pantalla.
2. En la pestaña "Acerca de", puede encontrar la versión en el campo "Número de

compilación".

¿Cómo resolvió el equipo de seguridad de ManageEngine esta vulnerabilidad?

@kuncho, un investigador de seguridad independiente, nos informó este problema el 12 de abril. Tan pronto como nos informaron de esto, se agregaron medidas de autenticación adecuadas para la llamada API y la última versión del producto con la solución, es decir, **NetFlow Analyzer v12.4.196** fue liberada el 22 de abril de 2020.

¿Cómo puedo identificar si mi instalación se ha visto comprometida?

1. Compruebe si hay nuevas cuentas de usuario de NFA que parezcan sospechosas, navegando a **Configuración> Configuración general> Administración de usuarios**. Si hay alguna, verifique que no haya sido creado por otros usuarios administradores (si corresponde) y elimine ese nuevo perfil de usuario de inmediato.
2. Además, puede verificar los logs de acceso para cualquier solicitud sendData no autenticada. En la carpeta "logs" en el directorio de instalación, abra **access_log.txt** y verifique si se ha realizado alguna de las siguientes llamadas API desde cualquier IP externa, es decir, sin el sufijo "- localhost" al lado de la dirección:
    i. sendData - se utiliza para exponer la clave de API al atacante.
    ii. addUser - posible acción de agregar usuario realizada utilizando la clave obtenida
    iii. testNProfile - posible RCE realizado en algunos / todos los dispositivos en la red

Si nota alguno de estos en su configuración, CIERRE INMEDIATAMENTE LA INSTALACIÓN y contacte a nuestro equipo de soporte.

¿Qué puedo hacer para corregir esta vulnerabilidad?

Si está en cualquier compilación de NetFlow Analyzer hasta la 12.4.195, se recomienda actualizar a NetFlow Analyzer v12.4.196 directamente desde nuestra página de service packs. Para los usuarios de NetFlow Analyzer versión 12.5, se recomienda actualizar a la compilación 12.5.120.

Alternativamente, también puede comunicarse directamente con nuestro equipo de seguridad para obtener ayuda con la actualización en itom-upgrades@manageengine.com o enviar una solicitud de soporte desde nuestra página de soporte para obtener asistencia de nuestros técnicos.

FIREWALL ANALYZER:

Subject line:
[CRITICO] Firewall Analyzer - Aviso de seguridad sobre CVE-2020-11946

Hola,

Saludos desde ManageEngine Firewall Analyzer. Este es un correo de aviso de seguridad que trata una **vulnerabilidad en la llamada sin autenticación al servlet** corregida en la última versión de Firewall Analyzer v12.4.196. SE RECOMIENDA ALTAMENTE que lea este correo para verificar si su instalación se ha visto afectada o no, y si está afectada, aprender a resolverla.

Nombre del problema y descripción:

Revelación de clave API no autenticada - Hubo un método de acceso no autenticado para obtener la clave API que se descubrió en el producto. El autor podría explotar esto para agregar un usuario administrador mediante una llamada a la API y realizar operaciones a nivel de administrador. Esta es una vulnerabilidad de seguridad **crítica**. (Consulte: CVE-2020-11946)

¿Quién ha sido afectado por esta vulnerabilidad?

Cualquier instalación de Firewall Analyzer con número de compilación entre **12.3.xxx y 12.4.195** (para FWA v12.3 y v12.4), y número de compilación entre **12.5.001 y 12.5.119** (para FWA v12.5) podría explotarse utilizando esta vulnerabilidad .

Si no está seguro en qué compilación se encuentra, puede encontrarlo fácilmente siguiendo estos pasos:

1. En el cliente web, haga clic en el icono Perfil en la esquina superior derecha de la

pantalla.
2. En la pestaña "Acerca de", puede encontrar la versión en el campo "Número de compilación".

¿Cómo resolvió el equipo de seguridad de ManageEngine esta vulnerabilidad?

@kuncho, un investigador de seguridad independiente, nos informó este problema el 12 de abril. Tan pronto como nos informaron de esto, se agregaron medidas de autenticación adecuadas para la llamada API y la última versión del producto con la solución, es decir, **Firewall Analyzer v12.4.196** fue liberada el 22 de abril de 2020.

¿Cómo puedo identificar si mi instalación se ha visto comprometida?

1. Compruebe si hay nuevas cuentas de usuario de FWA que parezcan sospechosas, navegando a **Configuración> Configuración general> Administración de usuarios**. Si hay alguna, verifique que no haya sido creado por otros usuarios administradores (si corresponde) y elimine ese nuevo perfil de usuario de inmediato.
2. Además, puede verificar los logs de acceso para cualquier solicitud sendData no autenticada. En la carpeta "logs" en el directorio de instalación, abra **access_log.txt** y verifique si se ha realizado alguna de las siguientes llamadas API desde cualquier IP externa, es decir, sin el sufijo "- localhost" al lado de la dirección:
    i. sendData - se utiliza para exponer la clave de API al atacante.
    ii. addUser - posible acción de agregar usuario realizada utilizando la clave obtenida
    iii. testNProfile - posible RCE realizado en algunos / todos los dispositivos en la red

Si nota alguno de estos en su configuración, CIERRE INMEDIATAMENTE LA INSTALACIÓN y contacte a nuestro equipo de soporte.

¿Qué puedo hacer para corregir esta vulnerabilidad?

Si está en cualquier compilación de Firewall Analyzer hasta la 12.4.195, se recomienda actualizar a Firewall Analyzer v12.4.196 directamente desde nuestra página de service packs. Para los usuarios de Firewall Analyzer versión 12.5, se recomienda actualizar a

la compilación 12.5.120.

Alternativamente, también puede comunicarse directamente con nuestro equipo de seguridad para obtener ayuda con la actualización en itom-upgrades@manageengine.com o enviar una solicitud de soporte desde nuestra página de soporte para obtener asistencia de nuestros técnicos.

OPUTILS:

Subject line:
[CRITICO] OpUtils - Aviso de seguridad sobre CVE-2020-11946

Hola,

Saludos desde ManageEngine OpUtils. Este es un correo de aviso de seguridad que trata una **vulnerabilidad en la llamada sin autenticación al servlet** corregida en la última versión de OpUtils v12.4.196. SE RECOMIENDA ALTAMENTE que lea este correo para verificar si su instalación se ha visto afectada o no, y si está afectada, aprender a resolverla.

Nombre del problema y descripción:

Revelación de clave API no autenticada - Hubo un método de acceso no autenticado para obtener la clave API que se descubrió en el producto. El autor podría explotar esto para agregar un usuario administrador mediante una llamada a la API y realizar operaciones a nivel de administrador. Esta es una vulnerabilidad de seguridad **crítica**. (Consulte: CVE-2020-11946)

¿Quién ha sido afectado por esta vulnerabilidad?

Cualquier instalación de OpUtils con número de compilación entre **12.3.xxx y 12.4.195** (para OpUtils v12.3 y v12.4), y número de compilación entre **12.5.001 y 12.5.119** (para OpUtils v12.5) podría explotarse utilizando esta vulnerabilidad .

Si no está seguro en qué compilación se encuentra, puede encontrarlo fácilmente siguiendo estos pasos:

1. En el cliente web, haga clic en el icono Perfil en la esquina superior derecha de la pantalla.
2. En la pestaña "Acerca de", puede encontrar la versión en el campo "Número de compilación".

¿Cómo resolvió el equipo de seguridad de ManageEngine esta vulnerabilidad?

@kuncho, un investigador de seguridad independiente, nos informó este problema el 12 de abril. Tan pronto como nos informaron de esto, se agregaron medidas de autenticación adecuadas para la llamada API y la última versión del producto con la solución, es decir, **OpUtils v12.4.196** fue liberada el 22 de abril de 2020.

¿Cómo puedo identificar si mi instalación se ha visto comprometida?

1. Compruebe si hay nuevas cuentas de usuario de OpUtils que parezcan sospechosas, navegando a **Configuración> Configuración general> Administración de usuarios**. Si hay alguna, verifique que no haya sido creado por otros usuarios administradores (si corresponde) y elimine ese nuevo perfil de usuario de inmediato.
2. Además, puede verificar los logs de acceso para cualquier solicitud sendData no autenticada. En la carpeta "logs" en el directorio de instalación, abra **access_log.txt** y verifique si se ha realizado alguna de las siguientes llamadas API desde cualquier IP externa, es decir, sin el sufijo "- localhost" al lado de la dirección:
    i. sendData - se utiliza para exponer la clave de API al atacante.
    ii. addUser - posible acción de agregar usuario realizada utilizando la clave obtenida
    iii. testNProfile - posible RCE realizado en algunos / todos los dispositivos en la red

Si nota alguno de estos en su configuración, CIERRE INMEDIATAMENTE LA INSTALACIÓN y contacte a nuestro equipo de soporte.

¿Qué puedo hacer para corregir esta vulnerabilidad?

Si está en cualquier compilación de OpUtils hasta la 12.4.195, se recomienda actualizar a OpUtils v12.4.196 directamente desde nuestra página de service packs. Para los

usuarios de OpUtils versión 12.5, se recomienda actualizar a la compilación 12.5.120.

Alternativamente, también puede comunicarse directamente con nuestro equipo de seguridad para obtener ayuda con la actualización en itom-upgrades@manageengine.com o enviar una solicitud de soporte desde nuestra página de soporte para obtener asistencia de nuestros técnicos.

OPMANAGER PLUS:

Subject line:
[CRITICAL] OpManager Plus - Aviso de seguridad sobre CVE-2020-11946

Hola,

Saludos desde ManageEngine OpManager Plus. Este es un correo de aviso de seguridad que trata una **vulnerabilidad en la llamada sin autenticación al servlet** corregida en la última versión de OpManager Plus v12.4.196. SE RECOMIENDA ALTAMENTE que lea este correo para verificar si su instalación se ha visto afectada o no, y si está afectada, aprender a resolverla.

Nombre del problema y descripción:

Revelación de clave API no autenticada - Hubo un método de acceso no autenticado para obtener la clave API que se descubrió en el producto. El autor podría explotar esto para agregar un usuario administrador mediante una llamada a la API y realizar operaciones a nivel de administrador. Esta es una vulnerabilidad de seguridad **crítica**. (Consulte: CVE-2020-11946)

¿Quién ha sido afectado por esta vulnerabilidad?

Cualquier instalación de OpManager Plus con número de compilación entre **12.3.xxx y 12.4.195** (para OpManager Plus v12.3 y v12.4), y número de compilación entre **12.5.001 y 12.5.119** (para OpManager Plus v12.5) podría explotarse utilizando esta vulnerabilidad .

Si no está seguro en qué compilación se encuentra, puede encontrarlo fácilmente

siguiendo estos pasos:

1. En el cliente web, haga clic en el icono Perfil en la esquina superior derecha de la pantalla.
2. En la pestaña "Acerca de", puede encontrar la versión en el campo "Número de compilación".

¿Cómo resolvió el equipo de seguridad de ManageEngine esta vulnerabilidad?

@kuncho, un investigador de seguridad independiente, nos informó este problema el 12 de abril. Tan pronto como nos informaron de esto, se agregaron medidas de autenticación adecuadas para la llamada API y la última versión del producto con la solución, es decir, **OpManager Plus v12.4.196** fue liberada el 22 de abril de 2020.

¿Cómo puedo identificar si mi instalación se ha visto comprometida?

1. Compruebe si hay nuevas cuentas de usuario de OpManager Plus que parezcan sospechosas, navegando a **Configuración> Configuración general> Administración de usuarios**. Si hay alguna, verifique que no haya sido creado por otros usuarios administradores (si corresponde) y elimine ese nuevo perfil de usuario de inmediato.
2. Además, puede verificar los logs de acceso para cualquier solicitud sendData no autenticada. En la carpeta "logs" en el directorio de instalación, abra **access_log.txt** y verifique si se ha realizado alguna de las siguientes llamadas API desde cualquier IP externa, es decir, sin el sufijo "- localhost" al lado de la dirección:
    i. sendData - se utiliza para exponer la clave de API al atacante.
    ii. addUser - posible acción de agregar usuario realizada utilizando la clave obtenida
    iii. testNProfile - posible RCE realizado en algunos / todos los dispositivos en la red

Si nota alguno de estos en su configuración, CIERRE INMEDIATAMENTE LA INSTALACIÓN y contacte a nuestro equipo de soporte.

¿Qué puedo hacer para corregir esta vulnerabilidad?

Si está en cualquier compilación de OpManager Plus hasta la 12.4.195, se recomienda

actualizar a OpManager Plus v12.4.196 directamente desde nuestra página de service packs. Para los usuarios de OpManager Plus versión 12.5, se recomienda actualizar a la compilación 12.5.120.

Alternativamente, también puede comunicarse directamente con nuestro equipo de seguridad para obtener ayuda con la actualización en itom-upgrades@manageengine.com o enviar una solicitud de soporte desde nuestra página de soporte para obtener asistencia de nuestros técnicos.