# BOLETÍN DE ALERTA

**Boletín Nro.**: 2022-15

**Fecha de publicación**: 03/03/2022

**Tema**: Múltiples vulnerabilidades en NGINX

**Softwares afectados:**

- Módulo NJS de NGINX versiones anteriores a la 7.0.2.

**Descripción:**

Se han publicado 4 (cuatro) vulnerabilidades en el módulo NJS de NGINX de criticidad alta, que permitirían a un atacante realizar ejecución remota de código (RCE), denegación de servicio (DoS), escalamiento de privilegios y corrupción de memoria en el sistema afectado. Se destacan las siguientes vulnerabilidades:

- CVE-2022-25139 de severidad crítica, con una puntuación de 9.8. Esta vulnerabilidad se debe a una falla en el componente *njs_await_fulfilled,* que permitiría a un atacante remoto realizar ejecución remota de código (RCE). La versión del software afectado es 0.7.0.

- CVE-2021-46463 de severidad crítica, con una puntuación de 9.8. Esta vulnerabilidad se debe a un error en el componente *njs_promise_perform_then*. Un atacante podría modificar el flujo de ejecución del programa con el objetivo de realizar escalamiento de privilegios o evadir controles de seguridad. La versión del software afectado es 0.7.1.

- CVE-2021-46461 de severidad crítica, con una puntuación de 9.8. Esta vulnerabilidad se debe a un error en el componente *njs_vmcode* que permitiría a un atacante realizar un ataque de denegación de servicio (DoS). La versión del software afectado es 0.7.0.

- CVE-2021-46462 de severidad alta, con una puntuación de 7.5. Esta vulnerabilidad se debe a un error en la función *njs_object_set_prototype* en el componente *njs_object,* que permitiría a un atacante provocar corrupción de memoria en el equipo afectado. La versión del software afectado es 0.7.1.

**Impacto:**

La explotación de estas vulnerabilidades permitiría a un atacante realizar ejecución remota de código (RCE), denegación de servicio (DoS), escalamiento de privilegios y corrupción de memoria en el sistema afectado.

**Detección:**

Verificar si se posee instalado la versión vulnerable del software en el equipo.

- Módulo NJS de NGINX versiones anteriores a la 7.0.2.

**Solución:**

Se recomienda instalar la versión más reciente proveída por el fabricante.

- https://docs.nginx.com/nginx/admin-guide/dynamic-modules/nginscript/

**Información adicional:**

- https://www.cert.gov.py/noticias/vulnerabilidad-use-after-free-uaf-detectada-en-modulo-njs-de-nginx
- https://nvd.nist.gov/vuln/detail/CVE-2021-46463
- https://nvd.nist.gov/vuln/detail/CVE-2022-25139
- https://nvd.nist.gov/vuln/detail/CVE-2021-46462
- https://nvd.nist.gov/vuln/detail/CVE-2021-46461
- https://security.netapp.com/advisory/ntap-20220303-0007/