Investigadores en ciberseguridad han identificado un nuevo fallo denominado «Día 0.0.0.0» que afecta a todos los principales navegadores web, lo que podría ser aprovechado por sitios maliciosos para comprometer redes locales.

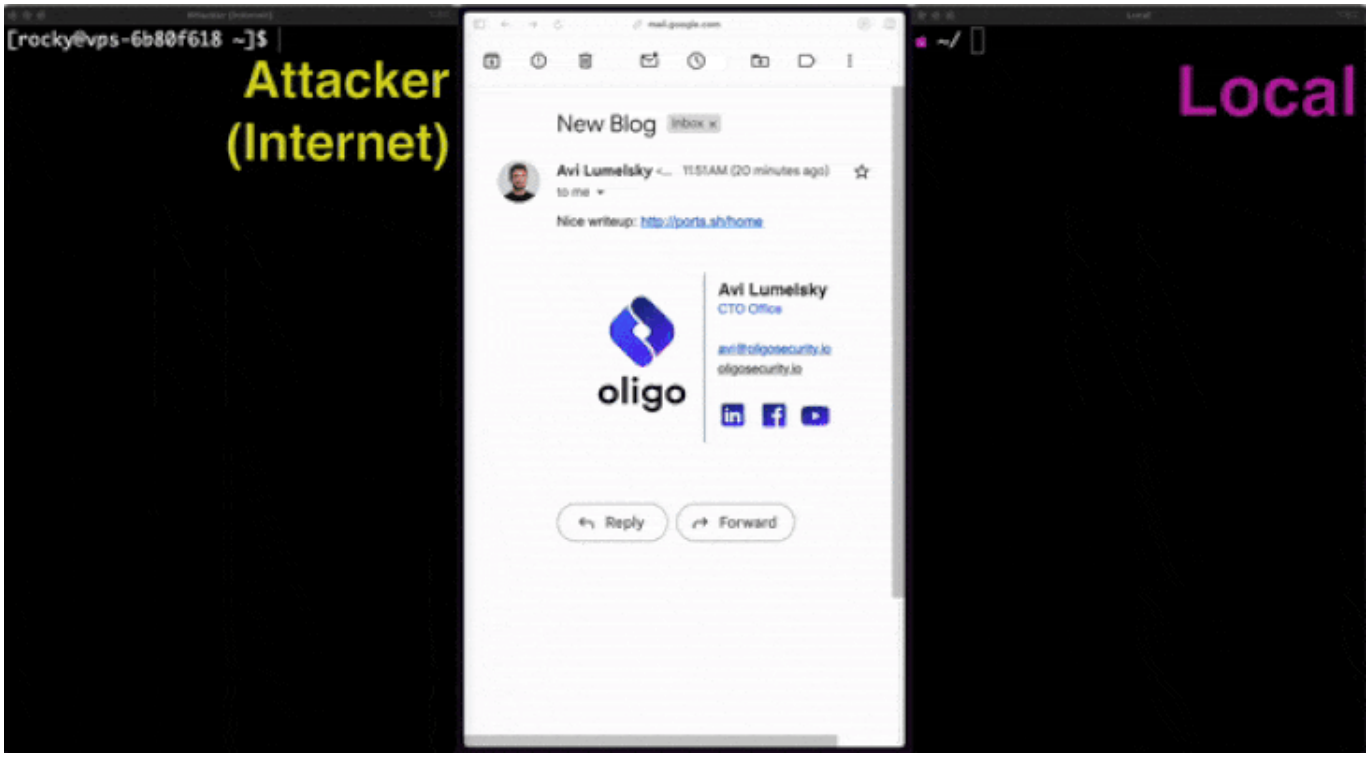
> Esta vulnerabilidad crítica *«revela un defecto fundamental en la manera en que los navegadores gestionan las solicitudes de red, lo que podría permitir a actores malintencionados acceder a servicios sensibles que se ejecutan en dispositivos locales,»* señaló Avi Lumelsky, investigador de Oligo Security.

La empresa israelí especializada en seguridad de aplicaciones destacó que las repercusiones de esta vulnerabilidad son significativas, y que se originan en la implementación inconsistente de mecanismos de seguridad y en la falta de estandarización entre diferentes navegadores.

Como consecuencia, una dirección IP aparentemente inocua, como 0.0.0.0, podría ser utilizada para explotar servicios locales, lo que resultaría en acceso no autorizado y en la ejecución remota de código por parte de atacantes fuera de la red. Se cree que esta vulnerabilidad ha estado presente desde 2006.

El «0.0.0.0 Day» afecta a Google Chrome/Chromium, Mozilla Firefox y Apple Safari, permitiendo que sitios web externos interactúen con software que se ejecuta localmente en MacOS y Linux. No afecta a dispositivos con Windows, ya que Microsoft bloquea la dirección IP a nivel del sistema operativo.

En particular, Oligo Security descubrió que sitios web públicos con dominios terminados en «.com» pueden comunicarse con servicios que se ejecutan en la red local y ejecutar código arbitrario en el sistema del visitante utilizando la dirección 0.0.0.0 en lugar de localhost/127.0.0.1.



Este hallazgo también elude la función de Acceso a Redes Privadas (PNA), diseñada para impedir que los sitios públicos accedan directamente a puntos finales dentro de redes privadas.

Cualquier aplicación que se ejecute en localhost y que sea accesible a través de 0.0.0.0 probablemente sea vulnerable a la ejecución remota de código, incluyendo instancias locales de Selenium Grid mediante el envío de una solicitud POST a 0.0.0[.]0:4444 con un payload diseñado específicamente.

Como respuesta a estos descubrimientos en abril de 2024, se espera que los navegadores web bloqueen completamente el acceso a 0.0.0.0, eliminando así el acceso directo a puntos finales de redes privadas desde sitios web públicos.

> *«Cuando los servicios usan localhost, asumen que se encuentran en un entorno*

> *restringido. Esta suposición, que en el caso de esta vulnerabilidad puede ser incorrecta, da lugar a implementaciones inseguras de servidores»,* explicó Lumelsky.
>
> *«Al utilizar 0.0.0.0 junto con el modo 'no-cors,' los atacantes pueden emplear dominios públicos para atacar servicios que se ejecutan en localhost e incluso lograr la ejecución arbitraria de código (RCE), todo ello mediante una única solicitud HTTP.»*