Nagios XI Stored Cross-Site Scripting (XSS): CVE-2021-38156

Unsupported Software & Unpatched Systems | Security Recommendations
Sep 17 | Written By Matt Mathur

Vulnerability Summary

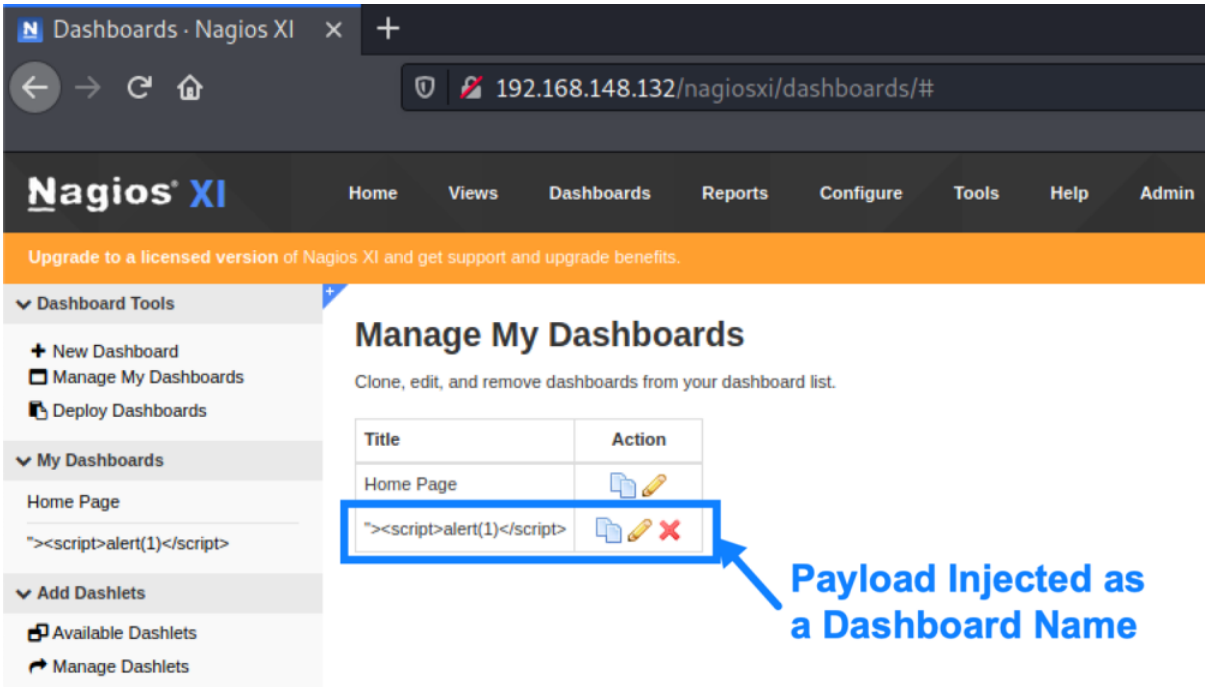
Recently, I discovered a stored cross-site scripting (XSS) vulnerability in Nagios XI v5.8.5. The vulnerability exists in the dashboard page of Nagios XI (/dashboards/#) when administrative users attempt to edit a dashboard. The dashboard name is presented back to the user unencoded when the edit button is clicked, which can allow dashboard names with malicious JavaScript to be executed in the browser.

Proof of Concept and Exploitation Details

The vulnerability can be triggered by inserting html content that contains JavaScript into the name field of dashboards. The following payload was used to launch an alert box with the number 1 in it as a proof of concept:

"><script>alert(1)</script>

An example of this in the dashboard's name field can be seen in the image below:



Above: Stored XSS Payload

After clicking the edit button for the dashboard name, the dashboard's name is loaded as unencoded HTML, as shown below:

Above: Unescaped JavaScript Tags

After clicking the edit button for the dashboard name, the JavaScript from the script tag is executed as shown in the following image:

Raxis discovered this vulnerability on Nagios XI v5.8.5.

Remediating the Vulnerability

Upgrade Nagios XI to version 5.8.6 or later immediately.

Disclosure Timeline

- **August 5, 2021** – Vulnerability reported to Nagios
- **August 6, 202**1 - CVE-2021-38156 is assigned to this vulnerability
- **September 2, 2021** - Nagios releases version 5.8.6 addressing this vulnerability

CVE Links and More

- **Mitre CVE** - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-38156
- **NVD** - https://nvd.nist.gov/vuln/detail/CVE-2021-38156

If you found this post interesting, please check out some others by and about Matt Dunn:

- Keep Your Cookies in the Cookie Jar: HttpOnly and Secure Flags
- Meet the Team: Matt Dunn, Lead Penetration Tester
- ManageEngine Applications Manager Stored Cross-Site Scripting Vulnerability (CVE-2021-31813)
- Remediating Account Enumeration Vulnerabilities

Matt Dunn | cross-site scripting | vulnerability management

Matt Mathur

Careers
Raxis News and Coverage
Raxis FAQ

Glossary
Boscloner
Meet the Raxis Team

LET'S TALK

Terms and Policies