

Multiple Vulnerabilities in Eyes of Network Web version 5.3

[← View More Research Advisories](#)

Synopsis

Several vulnerabilities have been discovered in the Eyes of Network web application. We have received no response from the vendor after repeated efforts to notify them of these vulnerabilities, and the application remains unpatched.

iFrame Injection

CVSSv3 Base Score: 7.3

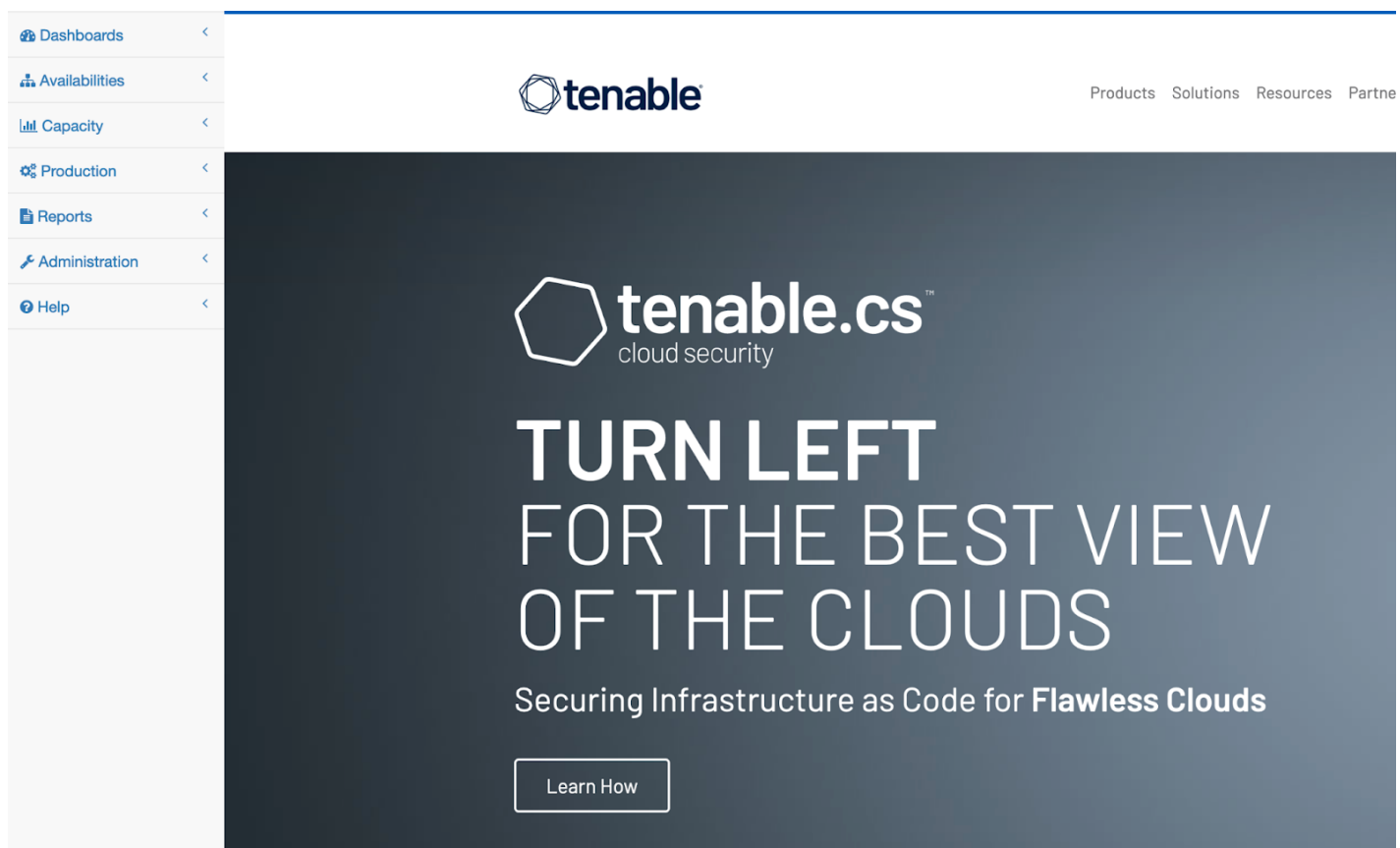
CVSSv3 Vector: AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:N

CWE: 74

The `url` parameter of `/module/module_frame/index.php` is vulnerable to iFrame injection. An attacker could use this issue to trick the user into loading remote malicious content into their authenticated session, which could allow the attacker to steal the user's credentials or force the client to carry out unwanted actions.

Proof of concept

After browsing to the URL shown below, an authenticated user will be greeted with the Tenable home page.



Cross-site Scripting via /module/admin_notifier/rules.php

CVSSv3 Base Score: 5.4

CVSSv3 Vector: AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N

CWE: 79

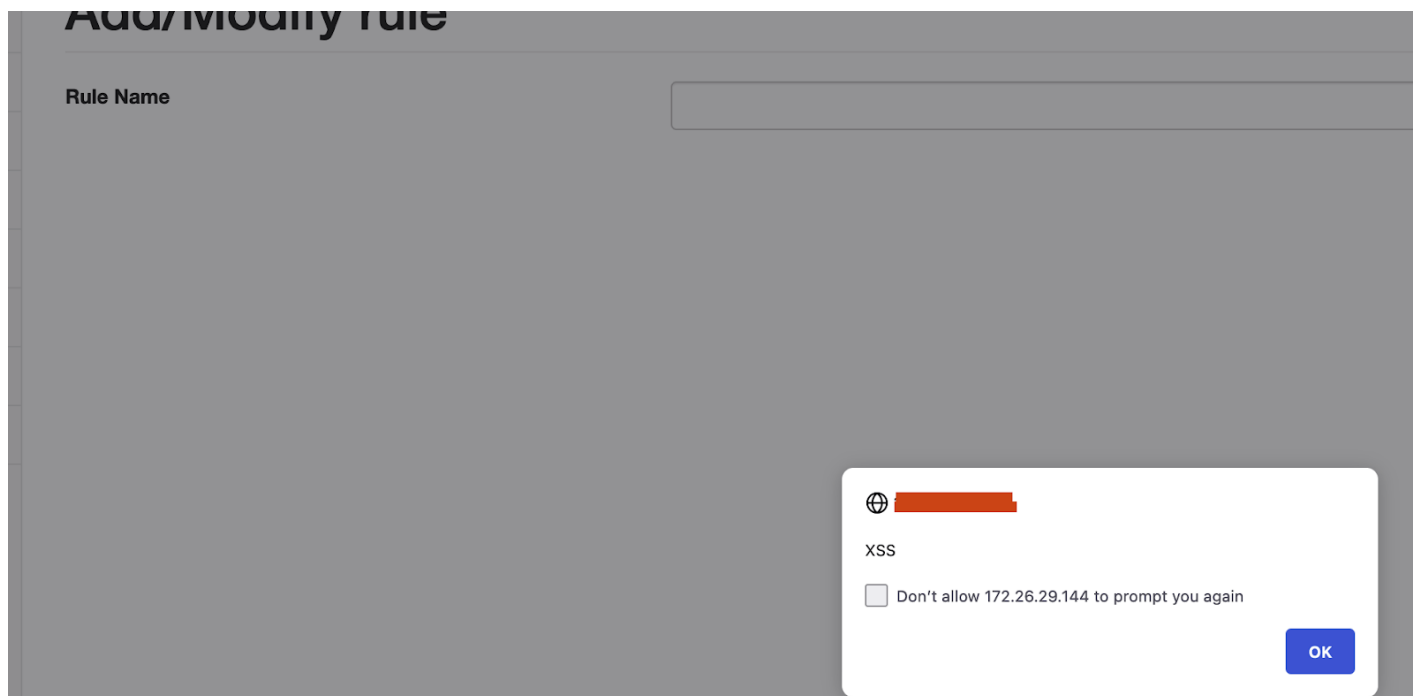
We have observed that the following parameters of rules.php are vulnerable to cross-site scripting attacks.

- rule_notification
- rule_name
- rule_name_old

An attacker could abuse this issue to trick an authenticated user into executing malicious Javascript.

Proof of Concept

If an authenticated user directs their browser to the URL, `https://<your-ip>/module/admin_notifier/rules.php?rule_name=%22%3E%3Cscript%3Ealert(%27XSS%27)%3C/script%3E`, then the Javascript expression `alert("XSS")` will be executed in their browser, displaying the message 'XSS':



Cross-site Scripting via /module/report_event/index.php

CVSSv3 Base Score: 5.4

CVSSv3 Vector: AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N

CWE: 79

The following parameters of index.php are vulnerable to cross-site scripting attacks:

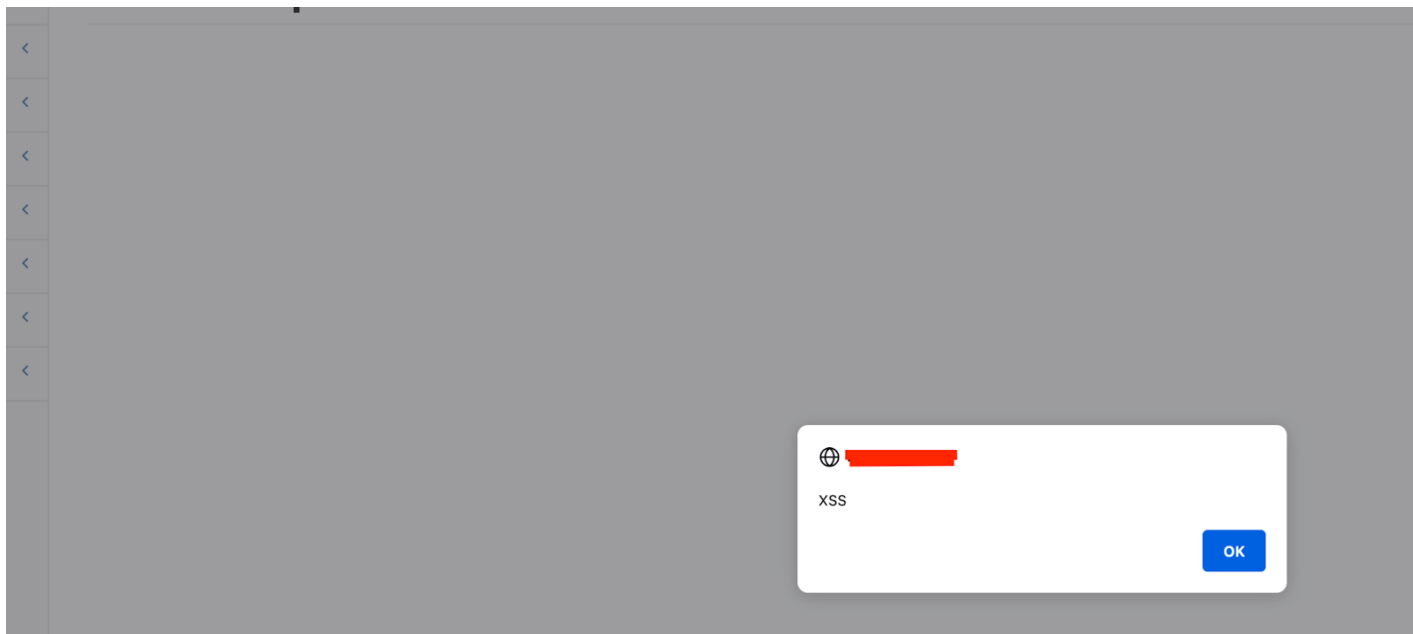
- rule_notification
- rule_name
- rule_name_old

An attacker could abuse this issue to trick an authenticated user into executing malicious Javascript.

Proof of Concept

Browsing to the URL `https:///module/report_event/index.php?`

`type=%22%3E%3Cscript%3Ealert(%27XSS%27)%3C%2Fscript%3E` as an authenticated user will cause the Javascript expression `alert("XSS")` to be executed in the browser, and will display the message "XSS".



Cross-site Scripting via /module/admin_user/add_modify_user.php

CVSSv3 Base Score: 5.4

CVSSv3 Vector: AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N

CWE: 79

The following parameters of **add_modify_user.php** are vulnerable to Cross Site Scripting:

- user_name
- user_mail

An attacker could abuse this issue to trick an authenticated user into executing malicious Javascript.

Proof of Concept

Browsing to the URL `https:///module/admin_user/add_modify_user.php?`

`user_name=%27%3E%3Cscript%3Ealert(%27XSS%27)%3C/script%3E` as an authenticated user will cause the Javascript expression `alert("XSS")` to be executed in the browser, and will display the message "XSS".

Cross-site request forgery

CVSSv3 Base Score: 6.3

CVSSv3 Vector: (AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:L)

CWE: 352

There is no CSRF protection within this application; we can see in the POST request below that there is no CSRF token being used.

```
POST /module/admin_user/add_modify_user.php HTTP/1.1
Host:
Cookie: glpi_dfa5b16f2330075f98b9929df5b4b397=6kijm2sinv45gcb9fp7g314bn1; PHPSESSID=af8p19dedugc1qoc1ltcc6gel6; ses
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 183
Upgrade-Insecure-Requests: 1

user_id=&user_name=hackerman&user_name_old=&user_mail=&user_descr=&user_password1=hackerman&user_password2=hackerman
```

An attacker could exploit this issue by creating a dummy page that would perform actions within an authenticated user's session if they were tricked into using the malicious dummy page.



DataTables_Table_0_length=10&user_selected%5B%5D=1&user_mgt_list=delete_user&action=submit as an authenticated user will delete the admin user.

Disclosure Timeline

Tuesday, June 21, 2022: Vendor Notified

Tuesday, July 15, 2022: Second Notification Sent to Vendor

Tuesday, August 5, 2022: Third and Final Notification Sent to Vendor

Monday, August 15, 2022: TRA Published

All information within TRA advisories is provided "as is", without warranty of any kind, including the implied warranties of merchantability and fitness for a particular purpose, and with no guarantee of completeness, accuracy, or timeliness. Individuals and organizations are responsible for assessing the impact of any actual or potential security vulnerability.

Tenable takes product security very seriously. If you believe you have found a vulnerability in one of our products, we ask that you please work with us to quickly resolve it in order to protect customers. Tenable believes in responding quickly to such reports, maintaining communication with researchers, and providing a solution in short order.

For more details on submitting vulnerability information, please see our [Vulnerability Reporting Guidelines](#) page.

If you have questions or corrections about this advisory, please email advisories@tenable.com

Risk Information

CVE ID: [CVE-2022-38357](#)

[CVE-2022-38358](#)

[CVE-2022-38359](#)

Tenable Advisory ID: TRA-2022-29

Credit: Derrie Sutton

CVSSv3 Base / Temporal Score: 7.3

CVSSv3 Vector: AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:N

Affected Products: Eyes of Network Web 5.3

Advisory Timeline

August 15, 2022: Initial Release

September 12, 2022: Corrected error in CVE number



Tenable.io Vulnerability Management

Tenable.io Web App Scanning

Tenable.asm External Attack Surface

Tenable.ad Active Directory

Tenable.ot Operational Technology

Tenable.sc Security Center

Tenable Lumin

Nessus

→ View all Products

FEATURED SOLUTIONS

Application Security

Building Management Systems

Cloud Security

Compliance

Exposure Management

Finance

Healthcare

IT/OT

Ransomware

State / Local / Education

US Federal

Vulnerability Management

Zero Trust

→ View all Solutions

CUSTOMER RESOURCES

Resource Library

Community & Support

Customer Education



[Nessus Resource Center](#)

[Cyber Exposure Fundamentals](#)

[System Status](#)

CONNECTIONS

[Blog](#)

[Contact Us](#)

[Careers](#)

[Investors](#)

[Events](#)

[Media](#)



[Privacy Policy](#) [Legal](#) [508 Compliance](#)

© 2022 Tenable®, Inc. All Rights Reserved

