# PRTG Network Monitor Stored Cross-Site Scripting Vulnerability (CVE-2021-29643)

Unsupported Software & Unpatched Systems | Security Recommendations
Aug 20 | Written By Matt Mathur

## Vulnerability Summary

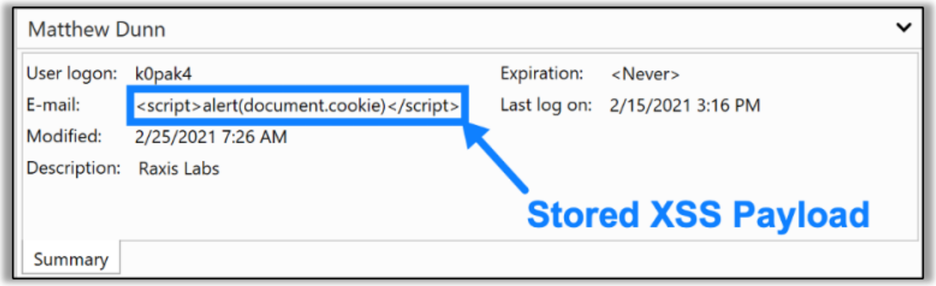
Recently, I discovered a stored Cross-Site Scripting vulnerability in PRTG Network Monitor Version 21.1.66.1623+. The vulnerability exists in the email field of user details on the "User Accounts" page at /systemsetup.htm?tabid=5 when users are loaded from Active Directory. After the page loads, the email field is loaded with unescaped content, allowing malicious JavaScript to be reflected back to the user.

## Proof of Concept and Exploitation Details

The vulnerability can be triggered by inserting HTML content, specifically script tags, into the email field of an Active Directory user. The following was inserted as a proof of concept to reflect the user's cookie in an alert box:

**<script>alert(document.cookie)</script>**

An example of this on one such user can be seen in the image below:

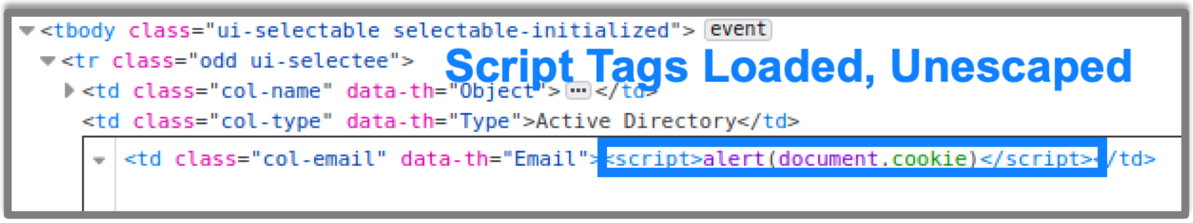


Matthew Dunn

User logon: k0pak4
E-mail: <script>alert(document.cookie)</script>
Modified: 2/25/2021 7:26 AM
Description: Raxis Labs
Expiration: <Never>
Last log on: 2/15/2021 3:16 PM

*Stored XSS Payload*

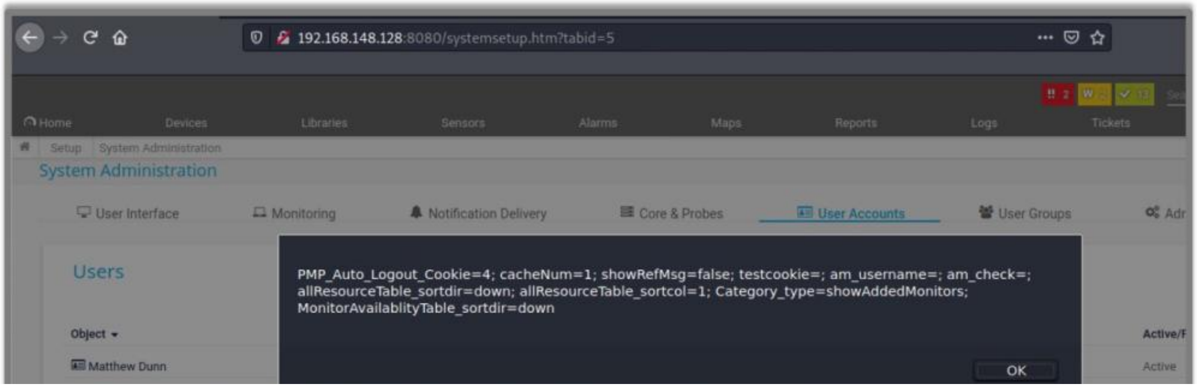
After loading the list of users, the HTML is then presented unescaped on the web page, which allows the script tags to be loaded as valid JavaScript. The unescaped HTML, as it loads in the browser, is seen in the next image:



```
▼<tbody class="ui-selectable selectable-initialized"> event
  ▼<tr class="odd ui-selectee">
    ▶<td class="col-name" data-th="Object">⋯</td>
     <td class="col-type" data-th="Type">Active Directory</td>
   ▼ <td class="col-email" data-th="Email"><script>alert(document.cookie)</script></td>
```

*Unescaped JavaScript Tags*

Once the page loads, the JavaScript executes, displaying the user's cookie to the screen, as shown in this picture:



192.168.148.128:8080/systemsetup.htm?tabid=5

```
PMP_Auto_Logout_Cookie=4; cacheNum=1; showRefMsg=false; testcookie=; am_username=; am_check=;
allResourceTable_sortdir=down; allResourceTable_sortcol=1; Category_type=showAddedMonitors;
MonitorAvailablityTable_sortdir=down
```

## Vulnerable Software Version

Raxis discovered this vulnerability on PRTG Network Monitor version 21.1.66.1623+.

## Remediating the Vulnerability

Upgrade PRTG Network Monitor to Version 21.3.69.1333 or later immediately. The release notes and upgrade instructions can be found here: https://www.paessler.com/prtg/history/stable#21.3.69.1333.

## Disclosure Timeline

- **March 22, 2021** – Vulnerability reported to Paessler Technologies.
- **March 25, 2021** – Vulnerability confirmed by Paessler Technologies.
- **April 12, 2021** - CVE-2021-29643 assigned to this vulnerability.
- **July 6, 2021** – Paessler releases version 21.3.69.1333 to address this vulnerability.

## CVE Links & More

- **Mitre CVE** - https://cve.mitre.org/cgi-bin/cvename.cgi?name= CVE-2021-29643
- **NVD -** https://nvd.nist.gov/vuln/detail/CVE-2021-29643

*If you're interested in this post, see more by and about Matt Dunn:*

- Meet the Team: Matt Dunn, Lead Penetration Tester
- At Raxis, Learning and Improving are Constants
- ManageEngine Applications Manager Stored Cross-Site Scripting Vulnerability (CVE-2021-31813)
- New Metasploit Module: Microsoft Remote Desktop Web Access Authentication Timing Attack

Share Tweet

Matt Dunn | cross-site scripting | vulnerability management

Matt Mathur

‹ Meet the Team: Adam Fernandez, Lead Developer

Meet the Team: Tim Semchenko, Senior Manager, Operations and Customer Delivery ›

©2022 Raxis LLC. 2870 Peachtree Road, Suite #915-8924, Atlanta, GA 30305