pfSense Packages - Feature #14696

possible cross site scripting and URL manipulation shell access injection issue sgerror.php

08/18/2023 10:33 PM - Jonathan Lee

Status:	Rejected	**Start date:**	
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	0%
Category:	squidguard	**Estimated time:**	0.00 hour
Target version:			
Plus Target Version:			

Description

Hello fellow pfSense Redmine team,

I seem to have found an issue with sgerror.php allowing a user to adapt the php file via the url after the error has already been displayed.

Ref:
https://forum.netgate.com/topic/182279/fixed-squidguard-redirect-page-for-error-codes-issues-with-https-ssl-interception/5?_=1692397066310

While researching a way to resolve my errors not displaying within SSL intercept I discovered that if a user sets Squidguard to use EXT URL MOVE and set the url to your internal url that points to sgerror.php I can possibly do command injection. Can this be set to have input validation?

History

#1 - 08/18/2023 10:48 PM - Jonathan Lee

if I can force it to say hello world, you could force it to say it a million times and do a denial of service attack in theory, or inject a shell program. I just thought it was weird we did adjustments like this in Cyber security class we would go through lists to test adjusting the URLS like this. My concern is it responded at all versus just having the input validation. Any thoughts here?

#2 - 08/18/2023 11:13 PM - Jonathan Lee

I wonder if there is any php injection vulnerabilities here. I did get it to say hello world. I noticed there is some CVEs listed for cross site scripting issues for pfsense, maybe it's issues like this that are being exploited. Again this would only be an issue if you have your management port open to all users.

#3 - 08/19/2023 12:02 AM - Jonathan Lee

- File Screenshot 2023-08-18 at 4.34.26 PM.png added

- File Screenshot 2023-08-18 at 4.59.48 PM.png added

sgerror.php is also still accessible even with the internal error redirector redirecting to external site like Google.com.

Please see attached photos

Redirector does direct also to Google now however I can still get to sgerror.php

This should in theory no longer be accessible if you are not using it or it is set to EXT URL.

#4 - 08/19/2023 12:03 AM - Jonathan Lee

In my case https://192.168.1.1:8080/sgerror.php?url=403%20Blocked%20by%20Mom%20and%20Dad&a=%a&n=%n&i=%i&s=%s&t=%t&u=%u was the url that could still be accessed and could be a php code script injection when GUI port is accessible.

#5 - 08/19/2023 12:05 AM - Jonathan Lee

/usr/local/www/sgerror.php

has no ability to disable internal error redirect functionality when utilizing external redirect.

#6 - 08/21/2023 01:52 PM - Jim Pingle

- Status changed from New to Rejected

That action is just echoing back the input to the user but as it passes through a query string and so on, the contents are not evaluated, only printed. It ends up encoded in a way that doesn't make it possible to execute anything. I tossed a bunch of different inputs at it (various PHP commands, exec commands, javascript tags, and so on) and thus far have been unable to produce anything other than benign output. Not even rendered HTML, just URL encoded strings.

It could maybe use an extra layer of encoding for safety but it doesn't appear to be critical unless it's something browser-specific that I've been unable to trigger.

Also in the future, this is ***NOT*** the place or method to report suspected security issues. Please report them responsibly as detailed on https://www.netgate.com/security and do not discuss them publicly.

#7 - 08/21/2023 02:01 PM - Jonathan Lee

Thanks for looking at this and testing the various inputs. I did not know about the other reporting URL I will use that next time.

Files

Screenshot 2023-08-18 at 3.23.56 PM.png	149 KB	08/18/2023	Jonathan Lee
Screenshot 2023-08-18 at 3.08.12 PM.png	421 KB	08/18/2023	Jonathan Lee
Screenshot 2023-08-18 at 4.34.26 PM.png	458 KB	08/18/2023	Jonathan Lee
Screenshot 2023-08-18 at 4.59.48 PM.png	200 KB	08/19/2023	Jonathan Lee