SΛFE

# LightSpeed Cache Vulnerability

## CVE-2020-29172

Nandini Rana Hanut Kumar Arora Shlok Gupta

www.safe.security

## **S** A F E

## Table of Contents

- INTRODUCTION
- XSS
- VULNERABILITY SEVERITY
- CVSS v3
- REMEDIATION
- EXPLOITATION
   Attack Scenario
   Exploitation
   Result
- **REFERENCES**



## Introduction

CVE-2020-29172 is a cross-site scripting (XSS) vulnerability. The Server IP option can be used to exploit cross-site scripting (XSS) vulnerability in the LiteSpeed Cache plugin for WordPress prior to 3.6.1.

The plugin does not sanitise invalid IPs given in its Toolbox page before displaying them in an error message which is Stored XSS.

The weakness was presented on 12/26/2020. This vulnerability is traded as CVE-2020-29172. The exploitability is said to be easy. It is possible to launch the attack remotely. The successful exploitation needs authentication and user interaction by the victim. This vulnerability is assigned to T1059.007 by the MITRE ATT&CK project.

Upgrading to version 3.6.1 eliminates this vulnerability.

#### XSS

XSS is the second most common problem in the OWASP Top 10, appearing in almost two-thirds of all applications. Some XSS issues may be detected automatically by automated techniques, particularly in established technologies like PHP, J2EE / JSP, and ASP.NET.

XSS has a mild impact for reflected and DOM XSS and a severe impact for stored XSS, involving remote code execution on the victim's browser, such as stealing passwords, sessions, or distributing malware to the victim.

The application or API saves unsanitized user input that may be accessed later by another user or an administrator. Stored XSS is frequently regarded as a high or critical risk.



## **Vulnerability Severity**

CVSS - 6.1 Medium

#### CVSS Vector - CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N

Attack Vector - Network

**Scope of Impact**- By executing script code in the user's current context, attackers can steal session cookies and perform session hijacking to impersonate the victim or take over their account and even more

**Risk** - Improper neutralization of input during web page generation effects plugins litespeed-cache

#### CVSS v3:

Base Score	6.1
Impact Score	2.7
Exploitability Score	2.8
Attack Vector (AV)	Network
Attack Complexity (AC)	Low
Privileges Required (PR)	None
User Interactions (UI)	Required
Scope (S)	Change
Confidentiality (C)	Low
Integrity (I)	Low
Availability (A)	None



## Remediation

The vulnerability is patched in version 3.6.1 of the LightSpeed Cache plugin.

## **Exploitation**

#### **Attack Scenario**

To demonstrate the attack we set up an **Apache2** server with **MySQL** on an Ubuntu Machine. We can see Apache2 and MySQL services running.







#### Next, we install WordPress on the Apache2 server

20 Applications	Places 😆 Firefox ESR	Dec 9 00:28		1 🗆 🕪 ტ
114		Dashboard (WordPress — WordPress	5 - Mozilla Firefox	_ • ×
Dashboard (WordPress -	V× +			
← → ୯ ଘ	👽 🔏 192.168.27.128/wp-admin/index.php			…⊙☆ ⊻⊪∖⊡ ◎ ≡
🐹 Kali Linux 🛛 🐹 Kali Too	is 🕱 Kali Forums 💆 Kali Docs 🤜 NetHunter 🧍 Offensive S	ecurity 🧍 MSFU 🖟 Exploit-DB 🌾 GHDB		
🚯 🏦 WordPress 😋 1	🛡 0 🕂 New 🚸			Howdy, admin 🖂
🚯 Dashboard 🔸	Dashboard			Screen Options 🔻 Help 🔻
Home	Dashboard			
Updates 📵	Welcome to WordPress			C Dismiss
	We've assembled some links to get you started:			
A Posts	Get Started	Next Stens	More Actions	
		Write your first blog post	Manage widgets	
Comments	Customize Your Site	+ Add an About page	Manage menus	
- Comments	or, <u>change your theme completely</u>	Set up your homepage	Turn comments on or off	
N Appearance		View your site	Learn more about getting started	
🖌 Plugins 📵				
👗 Users	Cite Haalth Ctatur	Outlet Deefe		
✗ Tools			i ii	
5 Settings	Site health checks will automatically run	Title		
Æ LiteSpeed Cache	No information yet periodically to gather information about your site. You can also <u>visit the Site</u>	Contract		
Collapse menu	Health screen to gather information about your site now.	What's on your mind?	I Drag boxes nere	Drag boxes here
			1 11	1
	Ata Glance A X A			1
		Save Draft	I	
	T 1Post IPage			
	WordPress 5.8.2 running Twenty Twenty-One theme	WordPress Events and News		
	Words read 5.0.2 forming <u>interest werky one</u> there.	Attend an upcoming event near you.		
	Activity	State of the Word Wednesday, Der 15, 2021		
	Recently Published	Online Wednesday, Dec 13, 2021		
SECOND STREET				
		- 🛅 🔁 🌛 🞱 🕂 🗸	9 🚯 🍎 🎹	



After installing and setting up WordPress on the Apache2 server we need to install the vulnerable plugin which is **LightSpeed Cache v.3.6 or lower** which can be downloaded from LightSpeed Cache site and then installed using zip-upload functionality of WordPress.:



Once our plugin is installed we can go to the **Toolbox** which has the vulnerable module under the **Debug Settings**.



Once our plugin is installed we can go to the **Toolbox** which has the vulnerable module under the **Debug Settings**.

a Applications	Plates					Toolbox ( Wordf	Press — Word	Press - Mozilla Fire	fox			
	No × +											
	Ø	2 192.168.27.128	wp-admin/admin.pl	p?page=litespe	ed-toolbox							
Kali Linux 🛛 📉 Kali To	ols 🛛 Kali For	ums 🧧 Kali Docs 🔇			MSFU 🦟 Explo	vit-DB 稀 GHDE						
🕆 WordPress 🖸	1 <b>9</b> 0 + 1	iew 🐵										Howdy, admin 💟
Dashboard	LiteSpee	d Cache Toolb	OX v3.6									
Posts	[1] Purge	[2] Import / Export	[3] Edit .htaccess	[4] Heartbeat	[5] Report [	6] Debug Settings	s [7] Log Vi	ew [8] Beta Test				
Media	ſ`											
Commonte	WARNIN	G										
Comments	LSCache	caching functions on this	page are currently unav	ailable!								
Appearance	> To us	e the caching functions y	ou must have a LiteSpee	d web server or be u	using QUIC.cloud CD	N. Learn More						
Plugins 📵												
Users	Purge	Learn More										
Tools												
Settings		Purge Front Page		Purge	Pages		403 P4	irge 403 Error	103	404	Purge 404 Error	
LiteSpeed Cache	-8	This was Purge Front Pag	e oray		u Purge Pages only		$\otimes$	rge error pages, includin	g +os pages	$\otimes$	Purge error pages, including 404 pag	
shboard												
nerai che	500	Purge 500 Error		Purge	All - LSCache		S-2 Pe	irge All - CSS/JS Cach	ne -	æ	Purge All - Opcode Cache	
N	8	Purge error pages, includ	ing 500 pages	by this	he LiteSpeed cache en plugin	tries created	S CS	is will purge all minified/ S/JS entries only	combined	8	Reset the entire opcode cache	
age Optimization												
ge Optimization		Purge All - Critical CS	s									
swier		This will delete all genera files	ited critical CSS									
olbox												
Collapse menu	B	Purge All		Empty	Entire Cache							
	8	Purge the cache entries of plugin except for Critical caches	reated by this CSS & LQIP	Clears a includi action s cached	all cache entries relate ing other web applica should only be used if t incorrectly.	d to this site, ations. This chings are						
					»-	- à 🕻	) M					

Once on the **Debug Settings** page, we can see there is a form which can be used to update settings by clicking on the **Save Changes** button.

		Toolbox (WordPress — WordPress - Mozilla Firefox		- 9
	Vor× +			
	0 🖉 192.168.27.128	wp-admin/admin.php?page=litespeed-toolbox#settings-debug	☺ ☆	
ali Linux 🛛 🗙 Kali Too	ils 📉 Kali Forums 🚊 Kali Docs 🕻			
☆ WordPress ⊕ 1	l 🛡 0 🕂 New 🛞			Howdy, admin
Dashboard	LiteSpeed Cache Toolb	<b>XX</b> v3.6		
Posts	[1] Purge [2] Import / Export	[3] Edit. htaccess [4] Heartbeat [5] Report [6] Debug Settings [7] Log View [8] Beta Test		
Media				
'ages	Debug Settings Learn Mo	ι.		Save Changes
Similar				
Appearance	Disable All Features	OFF ON		
lsers		This will disable LSCache and all optimization features for debug purpose.		
ools	Debug Log	orr ou Maria Boda		
lettings		Distructor WordPress dehua Ioa. To nerveral fillion un the disk this settion should be OFF when everything is working. The Admin IP notion will only output		
.iteSpeed Cache		log messages on requests from admin IPs. The logs will be output to wp-content/debug. Log.		
board	Admin IPs	101168.77.110		
iral.		and an a Million of indust		
5				
e Optimization				
Optimization base		Allows listed IPs (one per line) to perform certain actions from their browsers. Your IP: 192.168.27.129 More information about the available commands can be found here.		
ler				
xox	Debug Level	Basic Advanced		
ouapse menu		Advanced level will log more details,		
	Log File Size Limit	3 MB		
		Specify the maximum size of the log file. Recommended value: 3		
		🗊 늘 🗅 🦛 M 🍙 🖪 👍 :::		



The **Admin IPs** field is vulnerable to Stored XSS attack as there is no input validation done.

### **Exploitation**

To exploit this vulnerability, we will run BurpSuite, configure the browser's proxy accordingly and have it up and running.

Burg Suite Community Edition VOOL 5.2 - 1 emporary Project	Applications Places 🖡 burpsuite	Dec 9 00:31	1 •
rend rend rend rend rend rend rend rend rend	Project Infruder Repeater Window Help board Target Prov Intruder Repeater Sequencer Decoder Comparer Lo copt HTTP:history WebSockets.history Options	Burp Sulte Community Edition v2021.8.2 - Temporary Project gger Extender Project options Useroptions Learn	
Vew documentation       king burp Proxy       this is your first time using Burp, you might want to take a look at our guide to help you get the most out of your specificons.       Wew         Wew       Wew       Understand       Burp Proxy options       Reference information about the different options you have for castomizing Burp Proxy is behaviour.       View	Unread Drop Intercept is an Action Open Browser Use Burp's embedded browser There's no need to configure your proxy settings manuality. Use Burp's embedded Chromium browser to start testing right avey.	Use a different browser You'li need to perform a few additional steps to o proy settings for testing over HTTP's, you'l alor centitate	onfigure your browser's need to install Burgh CA
	Copen benever Using Burp Proxy If this is your first time using Burp, you might want to take a look at our guide to help you get the most out of your experiences. View	Were documentation           Burp Proxy options           Reference information about the different options you have for customizing Burp Proxy's behaviour.           View	Burp Proxy documentation The central point of access for all information you need to use Burp Proxy. View
		- 🔚 🗔 🌛 😂 🕅 🕂 🛃 🍎 🗄	



Once we have burp set up, we need to click on the **Save Changes** button on the **Debug Settings** page to see the request being made to the server.

en Applications Places ∎burpsuite Dec9 00:36 1 □ ♦ 0
Burp Suite Community Edition v2021.8.2 - Temporary Project _ 🛛 🗙
Burp Project Intruder Repeater Window Help
Dashbaard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn
/ request on thrijfys.ins.2/1.2/sou
Providence and the second
2 Host: 192.168.27.128
S USET-Agent: mOZILIG/S.0 (AI); LINUX X00_04; /V:/A0,0 USEK.02.000.001 /I/E0X/A.00 46 (Accept: text/html,xpl); application/xhtml+xml, app
5 Accept-Language: en-US, en 1,g=0.5 6 Accept-Language: en-US, en 1,g=0.5
7 Referer: http://192.168.27.128/wp-admin/admin.php?page=litespeed-toolbox
s content - type: application/x-www-form-untencoded 9 Content - Length: 603
10 Origin: http://192.168.27.128
12 Cookie: wordpress_d523ebfa57557c75758be6375b32d96f=admin%7C1640196890%7CMUE0q0QyGE1DZVrezDird3y0o2pgCUr2BarhFtmpdP%7C0bdcc5248bacf75326259cb0ae9f6233f580e496bffbfa6c5fa6b1f98a25df26;
<pre>Litespeed_tablesettings-debug; wordpress_test_cookie=w=%zwookie*vzvcneck; wordpress_iogged_in_dszeptra5/55/C/5/3bdeb3/505Zd951 admin%7C1840186809%70WEB0400yEC1DZvrezDir450X0gZpg0U728071703A790e1aabb544e5b3a6f9264b3a6af9263428b5acf20293c3d986fc88d; wp-settings-time-1=1638990321; _lscache_vary=</pre>
admin_bar%3A1%3B10gged_in%3A1%3Br01e%3A99 13.lborade_insecure.Pequests: 1
<pre>L3 L5/L9/L9/L9/L9/L9/L9/L9/L9/L9/L9/L9/L9/L9/</pre>
debug-filesize=36, settings-enroll%58%5D=debug-cookie=66, settings-enroll%58%5D=debug-collaps_qs&debug-collaps_qs=66_settings-enroll%58%5D=debug-inc&debug-i
()     ()    <
🕨 📩 🍋 M 🕢 🚯 🏎 📖





From the request we can see that Admin IPs field value is being sent for debug-ips parameter. We will try to send a URL encoded payload as value for this parameter which will trigger an XSS on the page.

#### Payload: <img src onerror=alert(/XSS/)>

URL Encoded: %3Cimg%20src%20onerror%3Dalert(%2FXSS%2F)%3E







#### <u>Result</u>

Once we forward the manipulated request to the server we can see a popup which is caused by the stored XSS.

a Applications	Places Firefox ESR		Dec 9 00:37		1 0 0 0
114		Toolbox ( W	ordPress — WordPress - Mozilla Firefox		- 0
Toolbox ( WordPress )	- × +				
) → × ŵ	🛛 🖉 192.168.27.128/wp-admin/admi	n.php?page=litespeed-toolbox		□ … ⊠ ☆	⊻ II\ CD &*
Kali Linux 🛛 🐹 Kali Tor	ols 📉 Kali Forums 🚆 Kali Docs 🧟 NetHunter 🔒 🤅	Offensive Security 🤰 MSFU 🦟 Exploit-DB 🌾 G	нов		
🕆 🖓 WordPress 🔿	1 🛡 0 🕂 New 🛞				Howdy, admin 🧾
Dashboard	Options saved.				
Posts	LiteSpeed Cache Toolbox				
Media	Entespeed Cache Toolbox 36				
Pages	[1] Purge [2] Import / Export [3] Edit .htacces	s [4] Heartbeat [5] Report [6] Debug Set	tings [7] Log View [8] Beta Test		
Comments	-				
400000000	WARNING				
Plugins (1)	LSCache caching functions on this page are currently of	navailablet	/xss/		
Users	> To use the caching functions you must have a Lites	peed web server or be using QUIC.cloud CDN. is			
Tools					
Settings	Purge Learn More		ок		
Litespeed Cache	Purge Front Page	Purge Pages	403 Purge 403 Error	Purge 404 Error	
shboard	- S This will Purge Front Page only				
the					
ns	Purge 500 Error	Purge All - LSCache	Purge All - CSS/JS Cache	Purge All - Opcode Cache	
age Optimization	Purge error pages, including 500 pages	Purge the LiteSpeed cache entries created by this plugin	This will purge all minified/combined     CSS/JS entries only	Reset the entire opcode cache	
ge Oppimization tabase					
wler.	Purge All - Critical CSS				
olbox	This will delete all generated critical CSS				
Collapse menu					
	Purge Att Purge the cache entries created by this	Ciears all cache entries related to this site,			
d 192.168.27.128	except for Critical CSS & LGIP	including other web applications. This			
		* * * * * * * * * * * * * * * * * * *	📣 M 👩 🗾 🥠		

When we click the **OK** button on the popup and go to the **Debug Settings** tab again, we can see that our payload (URL decoded) is in the **Admin IPs** field.

Applications	Places 🕑 Firefox ESR	Dec9 00:37	1 🗆 🖶 එ
114		Toolbox ( WordPress — WordPress - Mazilla Firefox	
	/ci× +		
) → ଫ ŵ	0 💋 192.168.27.12	8(vp-admin/admin.php?page=litespeed-toolbox 🖞 🚥 😇 😭	
🕻 Kali Linux 🛛 📉 Kali Tool	ls 🐹 Kali Forums 🧧 Kali Docs	🗙 NetHunter 🖡 Offensive Security 🗍 MSFU 🖟 Exploit-DB 烯 GHDB	
) 者 WordPress 😋 1	. 🗭 0 🕂 New 🚸		Howdy, admin 📔
Dashboard	LiteSpeed Cache Tool	box v3.6	
▶ Posts	Options saved.		0
] Media			
l Pages	[1] Purge [2] Import / Export	[3] Edit.htaccess [4] Heartbeat [5] Report [6] Debug Settings [7] Log View [8] Beta Test	
Comments			
Appearance	Debug Settings Learn M	tore	Save Changes
Plugins 🕕			
Users	Disable All Features	OFF ON	
" Tools		This will disable LSCache and all optimization features for debug purpose.	
Settings			
LiteSpeed Cache	Debug Log	OFF ON Admin IP Only	
hathboard		Outputs to WardPress debug leg. To prevent filling up the disk, this setting should be OFF when everything is working. The Admin IP option will anly output	
ieneral		log melsages on requests from admin ins. The logs will be output to up-concent/ oeoug, ( og .	
ache	Admin IPs	<img onerror="alerti//XSS/" src=""/>	
DN			
nage Optimization			
atabase			
rawler		Allows listed IPs (one per line) to perform certain actions from their browsers. Your IP: 192.168, 271.123	
xodloo		X invited Pr (). More information about the available commands can be found here.	
Collapse menu			
	Debug Level	Basic Advanced	
		Advanced level will log more details.	
		🔚 📩 🏟 M 🕂 🚯 🗰 🗰	



## References

- 1. https://nvd.nist.gov/vuln/detail/CVE-2020-29172
- 2. <u>https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-29172</u>
- 3. <u>https://wordpress.org/plugins/litespeed-cache/advanced/</u>
- 4. <u>https://wpscan.com/vulnerability/8ef35524-d996-4285-aca2-dc62e02c074d</u>





www.safe.security | info@safe.security

Palo Alto 3000, El Camino Real, Building 4, Suite 200, CA 94306