

#1516 Authenticated SQLi tại module news

URL / Location of vulnerability

http://nukeviethost/admin/index.php?my=news&op=adddtotopics

Description

Xin đọc pdf kèm theo về chi tiết của lỗi.

[Bug Disclosure Core.pdf](#)

Steps to reproduce

N/A

Impact

N/A

Recommendation


N/A

Attachments

 [POC-15161](#)

 **Ha Anh Hoang** created a report [3 years ago](#)


 **NukeViet** changed the status to **Resolved** [3 years ago](#)

 **NukeViet** added a comment [3 years ago](#)

Cảm ơn anh Hoàng đã đóng góp thông báo lỗi.
Chúng tôi đã sửa lỗi tại đây <https://github.com/nukeviet/nukeviet/commit/eda65a70932724887e6866014e36ed6d8ba5b6>
Ghi nhận của anh đã được cập nhật tại <https://github.com/nukeviet/nukeviet/blob/nukeviet4.3/CHANGELOG.txt#L6>
Phiên bản và lỗi sắp tới cũng sẽ được phát hành trong vòng tuần này hoặc tuần sau.
Một lần nữa xin cảm ơn anh!

 **Ha Anh Hoang** added a comment [3 years ago](#)


Cảm ơn vì đã resolve nhanh vấn đề. Sau khi bản cập nhật được phát hành tôi mong muốn được disclose báo cáo này để có thể xin cấp một CVE id mới. Liệu điều này là có thể trong tương lai hay không?


 **NukeViet** added a comment [3 years ago](#)

Gửi anh Hoàng,
Phần này trước giờ chúng tôi chưa thực hiện, nếu anh cần có thể nêu quy trình chúng tôi sẽ thực hiện.
Trước đây NukeViet cũng có công khai CVE ID ví dụ như <https://github.com/nukeviet/nukeviet/blob/nukeviet4.3/CHANGELOG.txt#L96> tuy nhiên ở lần đó tác giả cung cấp ID trước.

 **Ha Anh Hoang** added a comment [3 years ago](#)

Vậy lần này xin hãy đơn giản là phát hành bản và yêu cầu người sử dụng cập nhật. Sau một khoảng một tuần để đạt độ phổ biến nhất định, xin hãy disclose report này trên whitehub và có một public advisory về vấn đề này giống <https://nukeviet.vn/vi/news/Tin-an-ninh/huong-dan-fix-loi-bao-mat-cua-nukeviet-4-x-583.html>. Sau đó tôi sẽ liên lạc với Mitre để xin CVE Id. Thông tin cần phải Public trước khi có thể tạo một public CVE mới.

 **Ha Anh Hoang** requested to disclose this report [3 years ago](#)

 **NukeViet** added a comment [3 years ago](#)

Gửi anh Hoàng,
Theo như quy trình chúng tôi nhận được từ team quản lý của whitehub để disclose report và request CVE id thì thế này:
1. Request disclosure trên báo cáo này => Anh đã thực hiện
2. Bên em sau khi phát hành bản và khoảng 1 tuần sẽ disclose report và gửi anh link về bài thông báo trên trang chủ
3. Anh request CVE trực tiếp cho MITRE CVE và đính kèm link public của báo cáo này cùng thông báo changelog trên github của Nukeviet
4. Sau khi MITRE gán CVE ID anh gửi để bên em bổ sung vào changelogs của NukeViet

 **Ha Anh Hoang** added a comment [3 years ago](#)

Vâng, đó chính xác là những gì tôi đã đề xuất. Nếu không có gì khúc mắc thì xin hãy triển khai theo kế hoạch như vậy.

Program

NukeViet

Target

<https://github.com/nukeviet/>

Visibility

Public - Full

Status

Accepted - Resolved

Vulnerability

Server-Side Injection > SQL Injection

Severity

CRITICAL

Reference

#1516

Submitted at

12/12/2019 04:13:54

Submitted by

[Ha Anh Hoang](#)

Point

4

Votes

1

Public link

<https://whitehub.net/submissions/1516>

