bzyo Update README.md ... on Mar 25, 2021 History

..	
imgs	2 years ago
README.md	last year

README.md

Vulnerability

PacsOne Server 6.8.4 suffers from Incorrect Access Control.

Prerequisites

To successfully exploit these vulnerabilities, an attacker must be authenticated and have the ability to upload

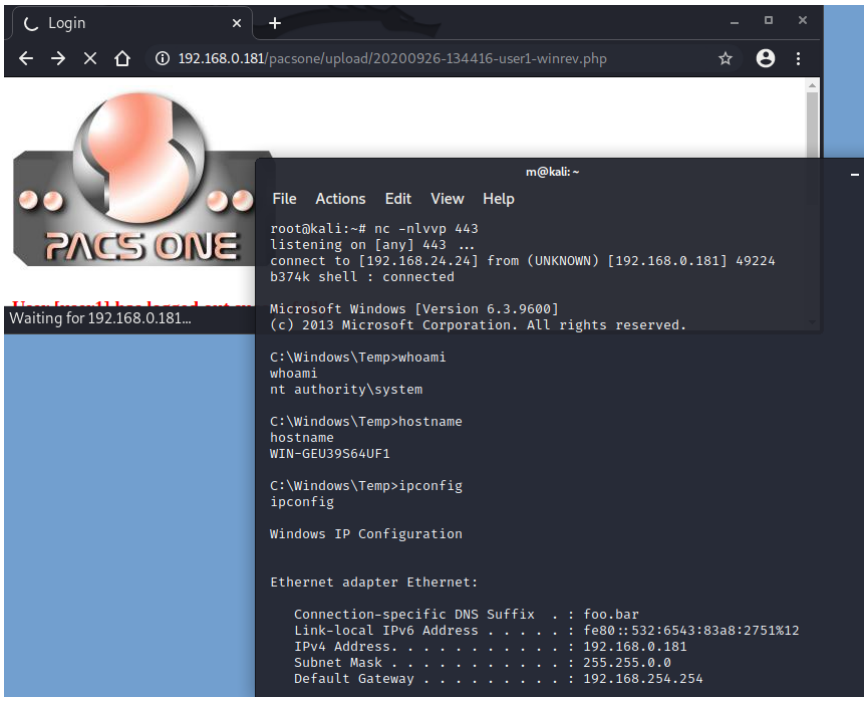
Exploit

The Dicom Image upload does not restrict file types allowing authenticated users with the ability to upload malicious code. While the upload folder does not list the files, the uploaded files are in a predicatable format as shown below.

```
Format:
date-time-username-filename.extension

Example:
20200926-134416-user1-winrev.php
```

An authenticaed or unauthenticaed user can access these files after upload and gain access to the system. Depending on how the web server is configured to run will determine what level of privileges to the server.



Timeline

05-07-20: Submitted incident through email, immediate response
05-21-20: Issue resolved
09-10-20: New version released
09-19-20: Submitted public disclosure

Reference

MITRE CVE-2020-12715

Disclaimer

Content is for educational and research purposes only. Author doesn't hold any responsibility over the misuse of the software, exploits or security findings contained herein and does not condone them whatsoever.