> Ghosts in the shell

.entry

Search

.entry
.articles
  .CVE-2025-63421
  .CVE-2025-61258
  .CVE-2023-27168
  .CVE-2023-27169
  .CVE-2023-27170
  .CVE-2023-27172
  .dllMemoryScanner
  .MessageBoxInjection
  .RtwqExecution
  .GuiCallbackHijack
  .avEvasion

.CVE-2023-27170
Vulnerability Overview
Context
What is Write-Back?
Technical description
Impact
Mitigation
Timeline
Credits

.CVE-2023-27170

Vulnerability Overview

Improper Limitation of a Pathname to a Restricted Directory.

Context

The vulnerability allows an attacker to change the directory to which an uploaded file is saved on the filesystem.

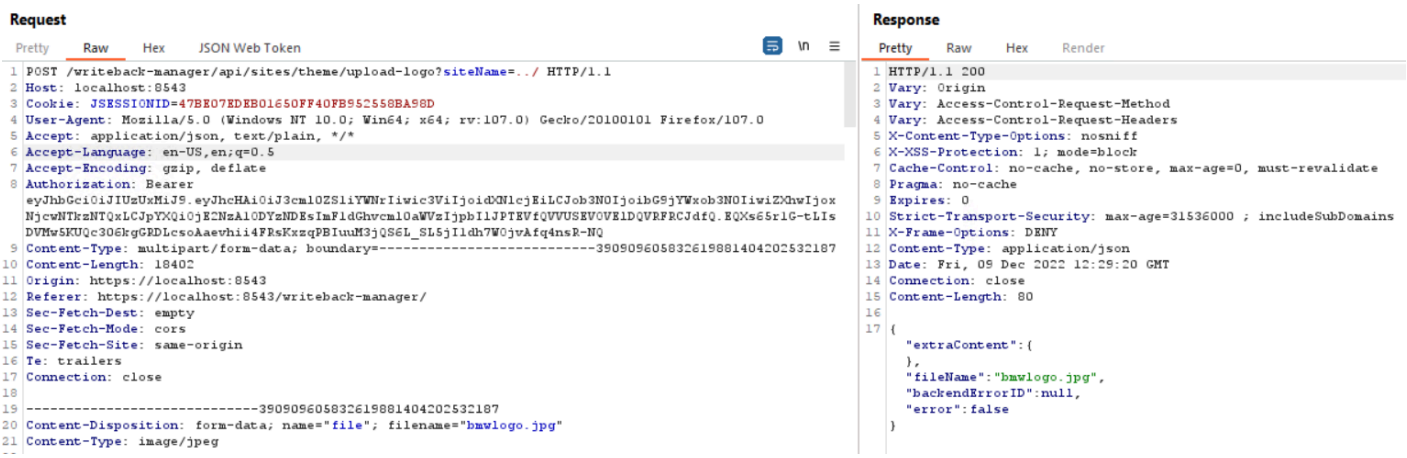
What is Write-Back?

Refer to Write-Back Description

Technical description

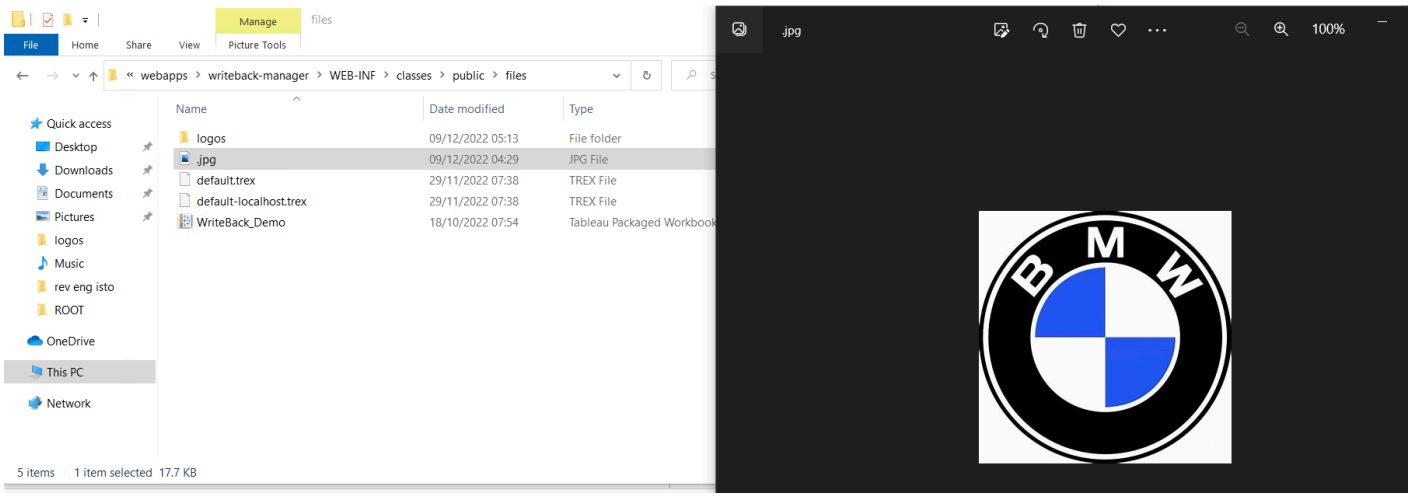
CVE-2023-27170 is a path or directory traversal security vulnerability, which allows an authenticated user to upload a file to any location on the file system, through any of the multiple file upload features on the Write-Back Manager.
This vulnerability was initially detected by changing the uploaded filename through a man-in-the-middle attack.

In the particular case of the customised logo upload (which was previously analysed in the blogpost regarding CVE-2023-27168), the name under which the logo file would be written to disk was the value passed in the siteName parameter, which by default was always `00000000-0000-0000-0000-000000000000`. By manipulating the value of this parameter and adding special characters such as dots '.' and slashes '/' an attacker can change the path to which the file will be written to:



In this example, the logo was placed one folder hierarchicaly above the logos

folder:



Impact

CVE-2023-27170 could be exploited in multiple manners. A malicious user could overwrite critical files, upload massive files causing a file space denial of service, upload dangerous files into the web tree in order to achieve code execution.

CVE ID: CVE-2023-27170
CVSS 3.1 Base Score: 5.5
CVSS Vector: AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:H/A:L
Affected Vendor: Xpand IT
Affected Product: Write-Back
Affected Version: Write-back Manager v2.3.1

Mitigation

Update Write-Back to at least version 4.1.

Timeline

12-12-2022 - Vulnerability detected and reported to Write-Back.
22-02-2023 - Vulnerability submitted to Mittre.
10-03-2023 - Vulnerability accepted and CVE ID reserved.
12-07-2023 - Official Patch released by Write-Back team.

Credits

me

Site built with MkDocs and Terminal for MkDocs.