Deloitte Risk Advisory Italia
VR Team

CREDITS: **Carlo Di Dato**

CASE NUMBER: **DVRT-2023-0001**

TITLE: **XAMPP for Windows insecure permissions**

CVE: **CVE-2022-47637**

SUMMARY

XAMPP for Windows Privilege Escalation

DESCRIPTION

URL: **https://www.apachefriends.org**

Software: XAMPP for Windows
Version: Up to 8.2.4
Vulnerable files:
xampp-windows-x64-8.2.0-0-VS16-installer.exe (MD5 - 3b2f32a9317ef0e4329f562c7f1b8e94)

- The installer in XAMPP through 8.2.0 allows local users to write to the C:\xampp directory. Common use cases execute files under C:\xampp with administrative privileges.
  The XAMPP installer creates the default folder "C:\xampp" and relative subfolders with insecure permissions. Specifically:

```
C:\>icacls C:\XAMPP
C:\ XAMPP BUILTIN\Administrators:(I)(OI)(CI)(F)
          NT AUTHORITY\SYSTEM:(I)(OI)(CI)(F)
          BUILTIN\Users:(I)(OI)(CI)(RX)
          NT AUTHORITY\Authenticated Users:(I)(M)
          NT AUTHORITY\Authenticated Users:(I)(OI)(CI)(IO)(M)

Successfully processed 1 files; Failed processing 0 files

C:\>
```

  as you can see, setting this permission to "NT AUTHORITY\Authenticated Users:(I)(OI)(CI)(IO)(M)" will allow any unprivileged authenticated user to modify, read and execute, list folder contents, read and write the folder.
  Since many XAMPP executables and batch files require administrative privileges (some of them can be install as Windows services), unprivileged users could overwrite legitimate files with malicious ones and subsequently elevate their privilege.

PROOF OF CONCEPT

Steps to reproduce the issue:

1. Install XAMPP for Windows
2. Check folder permissions

FIXES AND/OR MITIGATIONS

The issue can be mitigated by changing folders permissions.