

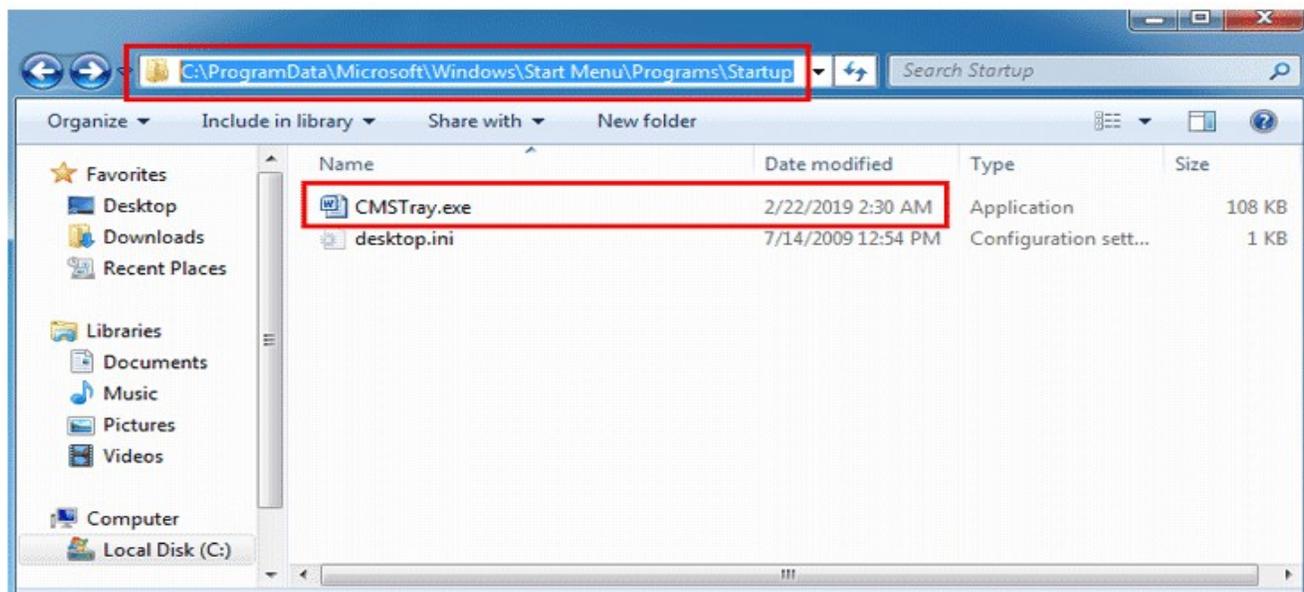
## WinRAR Flaw Being Exploited to Hack Windows Computers

Dear Constituents,

The popular windows file archival tool **WinRAR** has been in use for 19 years and it is used to view, create, pack and unpack archives in both ZIP and RAR formats. Beware Windows users of a new dangerous remote code execution vulnerability used by attackers to install malware within a victim's computer and gain complete control.

### How it works

- The flaw was a result of an Absolute Path Traversal bug that resides in the library called **UNACEV2.DLL**. (Dynamic Link Library).
- The **UNACEV2.DLL** is a third party library responsible for extracting archives in the ACE file format so the exploit has put over 500 million users around the world at risk.
- The vulnerability is being exploited by sending malspam (malware riddled emails) that contain CMSTray.exe, which is encapsulated within the malicious archiver instead of being downloaded remotely.
- As the victim opens the archive distributed by attackers, the malicious code is dropped into the startup folder (C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup\CMSTray.exe).



## What to do

- To all windows users are advised to update the application (WinRAR) immediately to the latest version (5.70 beta 2).
- Make sure to keep User Account Control (UAC) active if you are using an older version of WinRAR and avoid opening files received from unknown sources.

## Reference

- **Checkpoint:** <https://research.checkpoint.com/extracting-code-execution-from-winar/>

Please for more information you can contact us:

Tonga National CERT  
Ministry of MEIDECC  
Nuku'alofa  
Tel: 2378 (CERT)  
email: [cert@cert.gov.to](mailto:cert@cert.gov.to)  
web: [www.cert.gov.to](http://www.cert.gov.to)

### **Disclaimer Notice:**

The information in this notice is intended solely for public knowledge and awareness, and not intending to harm, fright or disturb any person(s), legal entity or the receiver of this information. Under no circumstances shall the Ministry of MEIDECC be liable for any indirect, incidental, consequential, special or exemplary damages arising out of or in connection with your access or use of or inability to access or use the information and any third party content and services