مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Privilege Escalation Vulnerability in Rufus

Tracking #:432318311

Date:26-01-2026

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a high-severity local privilege escalation vulnerability has been identified in Rufus, a widely used utility for creating bootable USB drives.

TECHNICAL DETAILS:

A high-severity local privilege escalation vulnerability has been identified in Rufus, a widely used utility for creating bootable USB drives. . The flaw, tracked as CVE-2026-23988, arises from a Time-of-Check Time-of-Use (TOCTOU) race condition in the handling of a PowerShell script (Fido) used for Windows ISO downloads. Due to unsafe file handling in the %TEMP% directory, a low-privileged local user can exploit this race condition to execute arbitrary code with Administrator privileges, effectively bypassing Windows User Account Control (UAC).

Vulnerability Details

- **CVE ID:** CVE-2026-23988
- **CWE:** CWE-367 – Time-of-Check Time-of-Use (TOCTOU) Race Condition
- **CVSS v3.1 Score:** 7.3 (High)
- **Product:** Rufus (Bootable USB creation utility)
- **Repository:** pbatard/rufus
- **Affected Versions:** All versions prior to 4.12
- **Patched Version:** 4.12

Impact:

Successful exploitation allows:

- Local privilege escalation from standard user to Administrator
- Execution of arbitrary commands with high integrity
- Potential installation of:
  - Malware
  - Backdoors
  - Persistence mechanisms

RECOMMENDATIONS:

- Immediate Actions: Upgrade Rufus to fixed version.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://github.com/pbatard/rufus/security/advisories/GHSA-hcx5-hrhj-xhq9