مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

High-Severity Vulnerability in Vim for Windows

Tracking #:432318098

Date:05-12-2025

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that a high-severity vulnerability has been identified in Vim allowing attackers to execute malicious code simply because a user opened a file in a compromised directory.

TECHNICAL DETAILS:

A high-severity vulnerability (CVE-2025-66476) has been identified in Vim for Windows versions prior to 9.1.1947. The flaw stems from an uncontrolled search path element (CWE-427), allowing arbitrary code execution when Vim, under Windows, resolves external commands from the current working directory before system paths. Attackers can exploit this by planting malicious executables inside a project directory, leading to execution with the user's privileges when Vim triggers external commands.

Vulnerability Overview

- CVE: CVE-2025-66476
- Severity: High
- CWE: CWE-427 – Uncontrolled Search Path Element
- Affected Versions: Vim for Windows < 9.1.1947
- Patched Version: 9.1.1947

RECOMMENDATIONS:

- Update Immediately-Upgrade Vim for Windows to fixed version or later.

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/vim/vim/security/advisories/GHSA-g77q-xrww-p834