



مجلس الأمن السيبراني
CYBER SECURITY COUNCIL



Critical Vulnerabilities in Ghostscript

Tracking #:432316498

Date:12-11-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical security update has been released for Ghostscript, a widely used open-source document rendering engine that processes PostScript and PDF files.

TECHNICAL DETAILS:

A critical security update has been released for **Ghostscript**, a widely used open-source document rendering engine that processes PostScript and PDF files. The new release (version 10.04.0) addresses multiple severe vulnerabilities, including remote code execution (RCE), buffer overflows, and path traversal risks. Exploiting these vulnerabilities could allow attackers to execute arbitrary code, access sensitive files, or cause denial-of-service conditions.

- CVE-2024-46951 and CVE-2024-46952: Unchecked pointers and buffer overflows lead to potential code execution.
- CVE-2024-46953 and CVE-2024-46956: Out-of-bounds memory access within Ghostscript's internal data structures, potentially causing corruption or arbitrary code execution.
- CVE-2024-46954: Directory Traversal via Overlong UTF-8 Encoding
- CVE-2024-46955: Out-of-Bounds Read Vulnerability

Fixed versions: Version 10.04.0 or Later

RECOMMENDATIONS:

The UAE Cyber Security Council recommends to install the fixed versions at the earliest.

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://ghostscript.com/releases/>