مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

Exploited Vulnerability in Ghostscript Library

Tracking #:432316033

Date:09-07-2024

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that a remote code execution vulnerability in the Ghostscript document conversion toolkit, widely used on Linux systems, is currently being exploited in attacks.

TECHNICAL DETAILS:

A remote code execution vulnerability in the Ghostscript document conversion toolkit, widely used on Linux systems, is currently being exploited in attacks. Ghostscript comes pre-installed on many Linux distributions and is used by various document conversion software, including ImageMagick, LibreOffice, GIMP, Inkscape, Scribus, and the CUPS printing system.

Vulnerability Details:

- **CVE-2024-29510** | CVSS score: 6.3 - Medium
- This format string vulnerability impacts all Ghostscript 10.03.0 and earlier installations. It enables attackers to escape the -dSAFER sandbox (enabled by default) because unpatched Ghostscript versions fail to prevent changes to uniprint device argument strings after the sandbox is activated.
- This security bypass is especially dangerous as it allows them to perform high-risk operations, such as command execution and file I/O, using the Ghostscript Postscript interpreter, which the sandbox would usually block.

Fixed Version:

- Ghostscript v10.03.1

RECOMMENDATIONS:

The UAE Cyber Security Council recommends updating the affected version to the fixed or latest versions released by Ghostscript.

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://nvd.nist.gov/vuln/detail/CVE-2024-29510/