computer
emergency
response
team
CERT-EU
for the EU institutions, bodies
and agencies

CERT-EU Security Advisory 2018-023

Major Vulnerability in Ghostscript

August 24, 2018 — v1.0

History:

- *24/08/2018 — v1.0: Initial publication*

Summary

Ghostscript – an interpreter for PostScript and PDF – is affected by a major vulnerability. There is currently no patch available, but some workarounds are possible.

Technical Details

Tavis Ormandy, a Google Project Zero security researcher, released details about a major vulnerability in Ghostscript [1]. To exploit this vulnerability, all an attacker needs to do is to send a specially crafted malicious file (which could be a PDF, PS, EPS, or XPS) to a victim, which, if opened with an application leveraging vulnerable Ghostscript, could allow the attacker to completely take over the targeted system [4].

Ghostscript suite includes a built-in `-dSAFER` sandbox protection option that handles untrusted documents, preventing unsafe or malicious PostScript operations from being executed. However, there are multiple `-dSAFER` sandbox bypass vulnerabilities, which could allow a remote, unauthenticated attacker to execute arbitrary commands on a vulnerable system [3].

There is currently no CVE for this vulnerability.

Products Affected

The Ghostscript interpreter is embedded in several operating systems, software suites, and libraries that allow desktop software and web servers to handle PostScript and PDF-based documents [2].

Recommendations

There is no solution for this issue for the moment. There is only the workaround mentioned below.

Workarounds

The researcher advise Linux distributions to disable the processing of PS, EPS, PDF, and XPS content until the issue is addressed [1].

For ImageMagick, an image processing library widely used in Linux, it is recommended to disable PS, EPS, PDF, and XPS coders in ImageMagick `policy.xml` [3]. ImageMagick uses Ghostscript by default to process PostScript content. ImageMagick can be controlled via the `policy.xml` security policy to disable the processing of PS, EPS, PDF, and XPS content. For example, this can be done by adding these lines to the `<policymap>` section of the `/etc/ImageMagick/policy.xml` file on a RedHat system:

```
<policy domain="coder" rights="none" pattern="PS" />
<policy domain="coder" rights="none" pattern="PS2" />
<policy domain="coder" rights="none" pattern="PS3" />
<policy domain="coder" rights="none" pattern="EPS" />
<policy domain="coder" rights="none" pattern="PDF" />
<policy domain="coder" rights="none" pattern="XPS" />
```

References

[1] http://openwall.com/lists/oss-security/2018/08/21/2

[2] https://www.kb.cert.org/vuls/byvendor?searchview&Query=FIELD+Reference=332928&SearchOrder=4

[3] https://www.kb.cert.org/vuls/id/332928

[4] https://www.bleepingcomputer.com/news/security/no-patch-available-yet-for-new-major-vulnerability-in-ghostscript-interpreter/