Secunia Advisory ID	SA84781
Title	Ghostscript Multiple Security Bypass Vulnerabilities
Release date	2018-08-21
Last update	2018-08-21
Criticality	- Highly critical
Impact	Security Bypass
Where	From remote
Solution Status	No Fix
Secunia CVSS Scores	CVSS3 Base: 9.8 , Overall: 9.0 CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:U/RC:C
CVE references	

Affected operating system and software

Software

Ghostscript 9.x

Advisory Details:

Description:

Multiple vulnerabilities have been reported in Ghostscript, which can be exploited by malicious people to bypass certain security restrictions.

1) An error when handling "/invalidaccess" checks can be exploited to bypass the -dSAFER functionality and subsequently inject and execute arbitrary shell commands via a specially crafted postscript file.

2) An error related to setpattern can be exploited to bypass the -dSAFER functionality and subsequently cause a segmentation fault via a specially crafted postscript file.

3) A type-confusion error related to LockDistillerParams can be exploited to bypass the -dSAFER functionality and subsequently cause a segmentation fault via a specially crafted postscript file.

4) An error related to .tempfile creation can be exploited to bypass the -dSAFER functionality and subsequently e.g. read and write arbitrary files via a specially crafted postscript file.

The vulnerabilities are confirmed in version 9.23. Other versions may also be affected.

Solution:

No official solution is currently available.

Provided and/or discovered by:

1-4) Tavis Ormandy, Google Project Zero.

Original advisory:

https://bugs.chromium.org/p/project-zero/issues/detail?id=1640
Tavis Ormandy:
http://seclists.org/oss-sec/2018/q3/142

References:

US-CERT:
https://www.kb.cert.org/vuls/id/332928

Changelog:

2018-08-21: Added a link to the "Original Advisory" section.
2018-08-21: Initial release