Vulnerabilities report

Evince (Poppler)

16/07/2015

I. Requester identification

Surname*	Levillain
Firstname*	Olivier
Organization / Company	ANSSI
Position in the organization	
Email address*	olivier.levillain@ssi.gouv.fr
Phone number	
Personal contact ?	No

II. Vulnerability reporter identification[1]

Surname*	Endignoux
Firstname*	Guillaume
Organization / Company	ANSSI
Position in the organization	Intern (april to july 2015)
Email address*	
Phone number	
Personal contact ?	

III. Vulnerabilities listing

A. Structure problems

Vulnerability identifier*	STRUCTURE
Editor*	Project Poppler
Relevant product(s) *	Evince
Relevant version(s) *	3.4.0 (Linux) using libpoppler 0.18.4
Description *	Some PDF structures are supposed to be trees. Yet, the syntax allows describing unconstrained oriented graphs. It is thus possible to create malformed files leading to a 100% CPU use or a segmentation fault. The folder “structure” contains several malformed files, which may lead to different interpretation from readers, since the specification does not really cover their content. In particular, the product will crash in presence of malformed destination name tree (“destname” and “destname-auto” files). It will use 100% CPU in presence of a malformed outline tree (“outlines*” files) or in presence of a malformed page labels tree (“pagelabels2” and “pagelabels3” files).
Class of vulnerability	Denial of service
Impact of the vulnerability	The program will consume a lot of CPU or crash.
Access vector	Local
Access complexity	Low
Authentication	None

[1] The person who has discovered the reported vulnerabilities

Confidentiality impact	None
Integrity impact	None
Availability impact	Complete
Indications to trigger the vulnerability*	Open the malformed file.
Comments	
CVE request*	Yes
TLP Level	**AMBER**

B. Name lax interpretation

Vulnerability identifier*	NAMES
Editor*	Project poppler
Relevant product(s) *	Evince
Relevant version(s) *	3.4.0 (Linux) using libpoppler 0.18.4
Description *	The product accepts invalid names (e.g. malformed escaped characters as in /Foo#0Z or long names). Instead of rejecting the file, it is rendered in a different way from other viewers (this particular example is “badescape”). Examples of malformed files are present in the “name” folder.
Class of vulnerability	Rendering error
Impact of the vulnerability	Possible confusion when opening a file (especially confusing in case of a signed file).
Access vector	Local
Access complexity	Low
Authentication	None
Confidentiality impact	None
Integrity impact	Partial
Availability impact	Partial
Indications to trigger the vulnerability*	Open the malformed file.
Comments	This vulnerability is far from critical.
CVE request*	No
TLP Level	**GREEN**

C. Generation number lax interpretation

Vulnerability identifier*	GENERATION
Editor*	Project Poppler
Relevant product(s) *	Evince
Relevant version(s) *	3.4.0 (Linux) using libpoppler 0.18.4
Description *	The product accepts invalid (e.g. negative) generation numbers in indirect object references instead of rejecting the file containing such malformed generation numbers. Examples of malformed files are present in the

	“generation” folder.
Class of vulnerability	Rendering error
Impact of the vulnerability	Possible confusion when opening a file (especially confusing in case of a signed file).
Access vector	Local
Access complexity	Low
Authentication	None
Confidentiality impact	None
Integrity impact	Partial
Availability impact	Partial
Indications to trigger the vulnerability*	Open the malformed file.
Comments	This vulnerability is far from critical.
CVE request*	No
TLP Level	**GREEN**

D. Number lax interpretation

Vulnerability identifier*	NUMBERS
Gnome Project ?	Project poppler
Evince	Evince
3.4.0 (Linux) using libpoppler 0.18.4	3.4.0 (Linux) using libpoppler 0.18.4
Description *	The product accepts invalid numbers (e.g. exponential forms, not allowed by PDF specification). Instead of rejecting the file, it is displayed (the interpretation being not always evident). Examples of malformed files are present in the “numbers” folder.
Class of vulnerability	Rendering error
Impact of the vulnerability	Possible confusion when opening a file (especially confusing in case of a signed file).
Access vector	Local
Access complexity	Low
Authentication	None
Confidentiality impact	None
Integrity impact	Partial
Availability impact	Partial
Indications to trigger the vulnerability*	Open the malformed file.
Comments	This vulnerability is far from critical.
CVE request*	No
TLP Level	**GREEN**