Bug 1900712 (CVE-2020-27778) - CVE-2020-27778 poppler: pdftohtml: access to uninitialized pointer could lead to DoS

Keywords: Security ×

Status: CLOSED ERRATA
Alias: CVE-2020-27778
Product: Security Response
Component: vulnerability
Version: unspecified
Hardware: All
OS: Linux
Priority: medium
Severity: medium
Target Milestone: ---
Assignee: Red Hat Product Security
QA Contact:
Docs Contact:
URL:
Whiteboard:
Depends On: ~~1900713~~ 1904080
Blocks: 1899505
TreeView+ depends on / blocked

Reported: 2020-11-23 15:10 UTC by Michael Kaplan
Modified: 2021-05-18 20:37 UTC (History)
CC List: 9 users (show)
Fixed In Version: poppler 0.76.0
Doc Type: If docs needed, set a value
Doc Text: A flaw was found in Poppler in the way certain PDF files were converted into HTML. This flaw allows a remote attacker to provide a malicious PDF file that, when processed by the 'pdftohtml' program, crashes the application, causing a denial of service. The highest threat from this vulnerability is to system availability.
Clone Of:
Environment:
Last Closed: 2021-05-18 20:37:13 UTC

Attachments	(Terms of Use)
Add an attachment (proposed patch, testcase, etc.)	

Michael Kaplan 2020-11-23 15:10:40 UTC — Description

In poppler-v0.75.0 in pdftohtml there is a buffer overflow.

Upstream issue:
https://gitlab.freedesktop.org/poppler/poppler/-/issues/742

Upstream fix:
https://gitlab.freedesktop.org/poppler/poppler/-/commit/30c731b487190c02afff3f036736a392eb60cd9a

Michael Kaplan 2020-11-23 15:11:04 UTC — Comment 3

Created poppler tracking bugs for this issue:

Affects: fedora-all [~~Bug 1900713~~]

Mauro Matteo Cascella 2020-12-03 09:29:45 UTC — Comment 6

This flaw revolves around the usage of the FILE pointer 'page' declared as a member variable of the HtmlOutputDev class. Under some circumstances this pointer is never initialized between the point in time when a HtmlOutputDev object is created and the time the same object is deleted. When the object is deleted, the destructor could use the same uninitialized pointer leading to undefined behavior (most likely a crash of the application).

```
/* class declaration */
class HtmlOutputDev: public OutputDev {
private:
  FILE *page;
};

/* destructor */
HtmlOutputDev::~HtmlOutputDev() {
  if (page != nullptr) {
    fputs("</body>\n</html>\n", page);   <= access to uninitialized pointer
  }
}
```

Mauro Matteo Cascella 2020-12-03 09:44:50 UTC — Comment 7

In reply to comment #0:
> Upstream fix:
> https://gitlab.freedesktop.org/poppler/poppler/-/commit/30c731b487190c02afff3f036736a392eb60cd9a

The patch initializes 'page' in the HtmlOutputDev constructor, effectively preventing the destructor from doing damage in case the pointer is never modified during the object's life cycle.

Mauro Matteo Cascella 2020-12-03 14:09:49 UTC — Comment 10

In reply to comment #6:
> This flaw revolves around the usage of the FILE pointer 'page' declared as a
> member variable of the HtmlOutputDev class. Under some circumstances this
> pointer is never initialized between the point in time when a HtmlOutputDev
> object is created and the time the same object is deleted. When the object
> is deleted, the destructor could use the same uninitialized pointer leading
> to undefined behavior (most likely a crash of the application).

Code execution might be possible, depending on the ability of the attacker to control and shape the heap state when the HtmlOutputDev destructor is executed. However, it does seem quite difficult to achieve and RHEL mitigations like ASLR would prevent this flaw from being exploited in any meaningful way.

errata-xmlrpc 2021-05-18 15:49:44 UTC — Comment 12

This issue has been addressed in the following products:

  Red Hat Enterprise Linux 8

Via RHSA-2021:1881 https://access.redhat.com/errata/RHSA-2021:1881

Product Security DevOps Team 2021-05-18 20:37:13 UTC Comment 13

This bug is now closed. Further updates for individual products will be reflected on the CVE page(s):

https://access.redhat.com/security/cve/cve-2020-27778

Note
You need to log in before you can comment on or make changes to this bug.