Bug report

林觀明

2022 / 3 / 10

OUTLINE

1. Bug Report
2. CVE ID Request
3. Example

Bug Report

- Report 需要什麼 ？
  - 版本
  - 怎麼重現
  - 平台
  - bug 細節

CVE ID

- CVE
  - 與資安相關的資料庫　收集漏洞並給予編號
  - https://cveform.mitre.org/
- CNA
  - CVE 編號的授權機構
  - https://www.cve.org/PartnerInformation/ListofPartners

CVE ID

Red Hat, Inc.

The majority of the links on this page redirect to external websites; these links will open a new window or tab depending on the web browser used.

Scope	Vulnerabilities in open-source projects affecting Red Hat offerings, that are not covered by a more specific CNA. CVEs can be assigned to vulnerabilities affecting end-of-life or unsupported Red Hat offerings
Program Role	CNA
Top-Level Root	**MITRE Corporation**
Security Advisories	**View Advisories**
Organization Type	Vendors and Projects
Country*	USA

* Self-identified by CNA

CVE ID

- How to request CVE ID
  - CVE（https://cveform.mitre.org/）
    - 可能會等很久
    - 如果是 CNA 的範圍的話，CVE 不會發
  - CNA
  - 可以請作者發 （作者有的不會發）

This is one of your vulnerability reports that would fall in the scope of Red Hat for assignment. To obtain CVE IDs through Red Hat, please extract all of those reports and place them in an email message to the secalert@redhat.com address.

CVE ID

林觀明 <p8706132@gmail.com>
发送至 secalert

Hi, I find 3 bugs in fribidi. I think it can affect this repo.
1. stack-buffer-overflow
https://github.com/fribidi/fribidi/issues/181
2. heap-buffer-overflow
https://github.com/fribidi/fribidi/issues/182
3. SEGV
https://github.com/fribidi/fribidi/issues/183

And also, I want to request CVE id.

Thanks and regards

CVE ID

- How to request CVE ID
  - CVE（https://cveform.mitre.org/）
    - 可能會等很久
    - 如果是 CNA 的範圍的話，CVE 不會發
    - 教學文： https://www.freebuf.com/articles/168362.html
  - CNA
  - 可以請作者發 （作者有的不會發）

This is one of your vulnerability reports that would fall in the scope of Red Hat for assignment. To obtain CVE IDs through Red Hat, please extract all of those reports and place them in an email message to the secalert@redhat.com address.

CVE ID

- 怎麼決定要發哪個呢？
  - Google target
  - 用之前的 cve 看是誰 assgin cve id
  - 如果都沒有先給 MITRE

CVE ID

CVE-ID

CVE-2020-35524 Learn more at National Vulnerability Database (NVD)
• CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information

Description

A heap-based buffer overflow flaw was found in libtiff in the handling of TIFF images in libtiff's TIFF2PDF tool. A specially crafted TIFF file can lead to arbitrary code execution. The highest threat from this vulnerability is to confidentiality, integrity, as well as system availability.

References

Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.

- CONFIRM:https://security.netapp.com/advisory/ntap-20210521-0009/
- URL:https://security.netapp.com/advisory/ntap-20210521-0009/
- DEBIAN:DSA-4869
- URL:https://www.debian.org/security/2021/dsa-4869
- FEDORA:FEDORA-2021-1bf4f2f13a
- URL:https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/BMHBYFMX3D5VGR6Y3RXTTH3Q4NF4E6IG/
- GENTOO:GLSA-202104-06
- URL:https://security.gentoo.org/glsa/202104-06
- MISC:https://bugzilla.redhat.com/show_bug.cgi?id=1932044
- URL:https://bugzilla.redhat.com/show_bug.cgi?id=1932044
- MISC:https://gitlab.com/libtiff/libtiff/-/merge_requests/159
- URL:https://gitlab.com/libtiff/libtiff/-/merge_requests/159
- MISC:https://gitlab.com/rzkn/libtiff/-/commit/7be2e452ddcf6d7abca88f41d3761e6edab72b22
- URL:https://gitlab.com/rzkn/libtiff/-/commit/7be2e452ddcf6d7abca88f41d3761e6edab72b22
- MLIST:[debian-lts-announce] 20210627 [SECURITY] [DLA 2694-1] tiff security update
- URL:https://lists.debian.org/debian-lts-announce/2021/06/msg00023.html

Assigning CNA

Red Hat, Inc.

Date Record Created

20201217 Disclaimer: The record creation date may reflect when the CVE ID was allocated or reserved, and does not necessarily indicate when this vulnerability was discovered, shared with the affected vendor, publicly disclosed, or updated in CVE.

Phase (Legacy)

Assigned (20201217)

CVE ID

- 怎麼決定要發哪個呢？

CVE-ID	
CVE-2021-45340	Learn more at National Vulnerability Database (NVD) • CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information
Description	
In Libsixel prior to and including v1.10.3, a NULL pointer dereference in the stb_image.h component of libsixel allows attackers to cause a denial of service (DOS) via a crafted PICT file.	
References	
Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.	
• MISC:https://github.com/libsixel/libsixel/issues/51	
Assigning CNA	
MITRE Corporation	
Date Record Created	
20211220	Disclaimer: The record creation date may reflect when the CVE ID was allocated or reserved, and does not necessarily indicate when this vulnerability was discovered, shared with the affected vendor, publicly disclosed, or updated in CVE.
Phase (Legacy)	
Assigned (20211220)	

Example

- libtiff: tiffcp
  - stack overflow
  - https://hackmd.io/@czzEsXJ_QH-KgrIp1RHWCQ/ByuPiVm-q