

Security Work & Process

How it works

Caolán McNamara

Principal Software Engineer

caolan.mcnamara@collabora.com



Collabora
Online



Technical Day
COOL
days





Terminology

CVE

- Common Vulnerabilities and Exposures
- A security flaw that's been assigned a CVE ID number

CNA

- CVE Numbering Authority
 - Mitre is the root and primary CNA
 - Various secondary CNAs that can assign CVE IDs for other products
 - And CNAs that assign CVEs for their own products

EMBARGO

- CVE assigned, but not yet public

CWE

- Common Weakness Enumeration. Common causes, patterns

CVSS

- Common Vulnerability Scoring System. How bad is it.



Collabora Online Process

Collabora Online uses github as CNA

- Github does the assigning on behalf of CO
- Using the github integrated security process
 - Request a CVE from github
 - They review and assign
 - Embargo is delegated to the project

The screenshot shows the GitHub interface for the 'CollaboraOnline / online' repository. The 'Security' tab is selected, displaying 'Security Advisories'. The page includes a search bar, navigation links for Code, Issues (625), Pull requests (69), Discussions, Actions, Projects (1), Security (395), Insights, and Settings. A sidebar on the left shows navigation options: Overview, Reporting, Policy, Advisories (11), and Vulnerability alerts. The main content area shows a summary of security advisories: 1 Triage, 0 Draft, 11 Published, and 0 Closed. A specific advisory is highlighted: 'CVE-2024-29182 Stored Cross-Site-Scripting vulnerability via tooltip', with details 'GHS-9gmw-5q2c-4398 published 1 hour ago by caolanm' and a 'High' severity rating. A green button 'New draft security advisory' is visible in the top right corner.



Open a draft security advisory

After the draft security advisory is open, you can privately discuss it with collaborators and create a temporary private fork where you can collaborate on a fix. If you've already fixed the vulnerability, just fill out the draft security advisory and then publish it.

Advisory Details

Title *

CVE identifier

Request CVE ID later

Description *

Write

Preview

H

B

I

≡

<>

🔗

≡

≡

≡

📎

←

Impact

What kind of vulnerability is it? Who is impacted?

Patches

Has the problem been patched? What versions should users upgrade to?

Workarounds

Is there a way for users to fix or remediate the vulnerability without upgrading?

Access and visibility

Until it is published, this draft security advisory will only be visible to collaborators with admin permissions on **CollaboraOnline/online**. Other users and teams within the organization may be added once the advisory is created.

Once published, security advisories on public repositories are visible to everyone.

Once reviewed by GitHub, security advisories may be broadcast on the [GitHub Advisory Database](#). They may also trigger Dependabot alerts to users that depend on this repository.

🔒 Security policy

📖 Glossary and documentation



Collabora Online Process

Collabora Online uses github as CNA

- Fill in the form, description, versions affected, fixed, etc
- Can use the integrated CVSS calculator to generate a severity
- Can add reporter as collaborator if they have a github account
- Request a CVE
- When assigned, can publish
- Advisories published at
 - <https://github.com/CollaboraOnline/online/security/advisories?state=published>



LibreOffice Process

The Document Foundation is the CNA for LibreOffice

- So third parties don't issue CVEs
- Red Hat is "Root" for TDF
 - Lack of response, appeals that a CVE wasn't assigned, etc
 - CNA picks their root
- I happen to be the representative there
 - Holder of CVE API token `CVE_API_KEY`



LibreOffice Process

“cve” command line tools

- cve list
- cve reserve
- cve publish

```
caolan@fedora:~$ cve list
```

CVE ID	STATE	OWNING CNA	RESERVED BY	RESERVED ON
CVE-2019-9847	PUBLISHED	Document Fdn.	REDACTED (Document Fdn.)	Sun Mar 17 00:00:00 2019 +0000
CVE-2019-9848	PUBLISHED	Document Fdn.	REDACTED (Document Fdn.)	Sun Mar 17 00:00:00 2019 +0000
CVE-2019-9849	PUBLISHED	Document Fdn.	REDACTED (Document Fdn.)	Sun Mar 17 00:00:00 2019 +0000
CVE-2019-9850	PUBLISHED	Document Fdn.	REDACTED (Document Fdn.)	Sun Mar 17 00:00:00 2019 +0000
CVE-2019-9851	PUBLISHED	Document Fdn.	REDACTED (Document Fdn.)	Sun Mar 17 00:00:00 2019 +0000
CVE-2019-9852	PUBLISHED	Document Fdn.	REDACTED (Document Fdn.)	Sun Mar 17 00:00:00 2019 +0000
CVE-2019-9853	PUBLISHED	Document Fdn.	REDACTED (Document Fdn.)	Sun Mar 17 00:00:00 2019 +0000
CVE-2019-9854	PUBLISHED	Document Fdn.	REDACTED (Document Fdn.)	Sun Mar 17 00:00:00 2019 +0000
CVE-2019-9855	PUBLISHED	Document Fdn.	REDACTED (Document Fdn.)	Sun Mar 17 00:00:00 2019 +0000



LibreOffice Process

Publishing

- JSON “CVE” format
 - I use <https://vulnogram.github.io/> to generate it
- Previously CVE 4 format, submitted through
 - <https://cveform.mitre.org/>
 - Limited in length, had to minify json, nightmare fuel
- Now CVE 5 format, submitted through
 - `cve publish -f CVE-whatever.json`
- “publish” takes json format, now needs “CVE 5” format

Advisories

- <https://www.libreoffice.org/about-us/security/advisories/>



NEW

Open

Download

Post to CVE.org

CVE-yyyy-nnnn..

Load

Editor

6

Source

Preview

CVE Portal

CVE ID *

CVE-yyyy-nnnn or pick from existing

cve.org

Enter CVE-yyyy-nnnn format.

Title

eg., Memory leak in Linux Filesystem

Public at

dd / mm / yyyy , -- : --

Problem types

eg., CWE-20 Improper Input Validation

Impacts

eg., CAPEC-130 Excessive Allocation

+ Problem type

+ Impact

Affected products *

Enter a vendor and product OR a package and a collection

Vendor or project

eg., Linux

Product name

eg., Linux Kernel

Platforms

eg., x86, Android, Windows, MacOS, ..

Package collection URL

eg., https://wordpress.org/plugins

Package name

eg., kernel

Source repository (OSS)

eg., https://git.kernel.org

Modules, components, or features

eg., filesystem

Source-code file (OSS)

eg., hello.c

Program routines (OSS)

+ Program routine

Versions (exact versions or ranges)



Common Reporting Process

Reporting

- Reports to officesecurity@lists.freedesktop.org
- Shared list for basically projects with a StarOffice lineage
 - LibreOffice, Apache OpenOffice, Collabora Office, Collabora Online, etc.
- Policy is to disclose the vulnerability to the public within 30 days of resolution of the issue
- Reports will be credited in security advisories, but reporters may remain anonymous if they wish



Common Process

Reporting, Triage, Crediting

- What projects does it affect
 - Is there a need to coordinate a common embargo date
- Is it in a third party module
 - Typically request a CVE through our root CNA if so
- What embargo date to use
 - Try and balance getting a timely fix, existing release schedules, reporters desire not to lose their exclusivity to another less principled reporter
- Crediting
 - Kudos is typically all we have to offer. Important to give credit in reporters preferred form

Fixing them is important too


- Thanks to reporters for doing the reporting responsibly
- Thanks to all at Collabora Productivity, allotropia and Red Hat for providing fixes
- Thanks to maintainers of 3rd party software for above and beyond help. HSQLDB, XMLSec, etc.



Collabora
Online



LibreOffice Technology

Technical Day
COOL
days 

Thank you!



@CollaboraOffice
hello@collaboraoffice.com
www.collaboraoffice.com