Security Work & Process How it works

Caolán McNamara

Principal Software Engineer caolan.mcnamara@collabora.com











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.

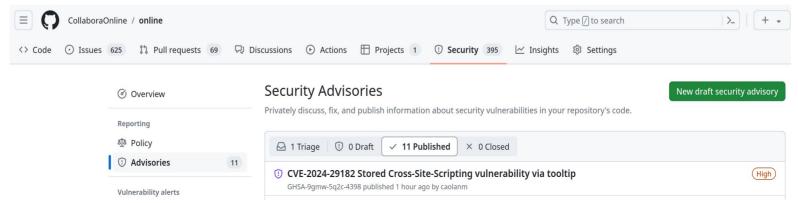




Collabora Online Process

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







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.

/E identifi								
	er							
Request C	VE ID later	\$						
	T.							
escription	*							
Write	Preview	HE	3 <i>I</i>	i= <>	8	$\stackrel{1}{2}\equiv \stackrel{:}{\equiv}$	ΔΞ	0
### Impa			,,	. 12				
what kin	id of vulnerabi	lity is it? V	/ho is in	npacted?	-			
### Patch	201							
	163							

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.



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						
U				<u> </u>						





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

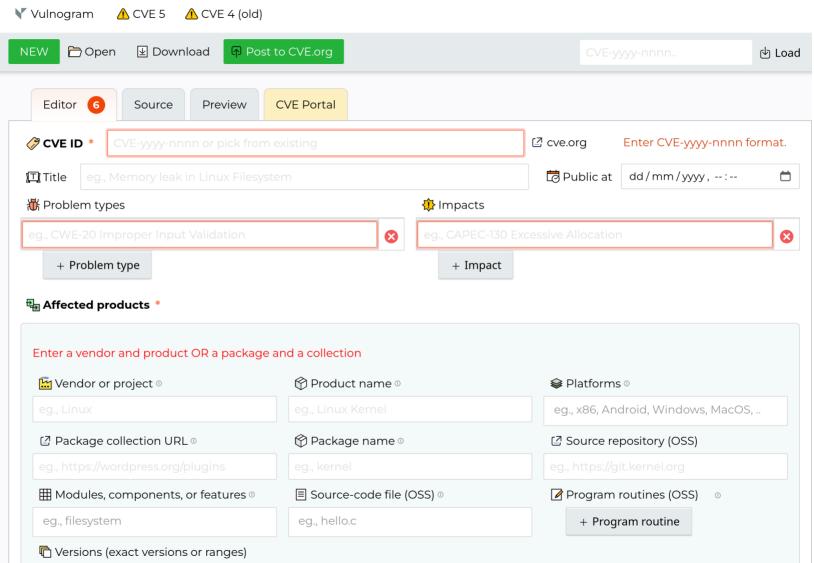
Advisories

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













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





Thank you!









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