

Using Vulnogram with CVE Services

Last Updated: 2024-04-11¹

1 Overview	2
Quick Start	2
2 Terminology	2
3 Becoming a CVE Numbering Authority (CNA)	3
4 Getting CVE Services Credentials	3
Test Credentials	3
Production Credentials	3
5 Vulnogram	4
Getting Started	4
CVE Portal Tab	4
Editor Tab	5
Source Tab	5
Preview Tab	6
6 User Management	6
Create a User	6
Change User Information	8
User ID	8
User Name	10
Reset API Key	11
Manage Administrators	13
Disable and Enable Users	14
7 CVE Record Management	15
QuickStart - Reserving, Populating, and Posting a CVE Record	15
Reserve a CVE ID	16
Populate (Write) a CVE Record	16
Required Elements	17
CVE ID	17
Affected Products	18
CVE Description	19
Reference(s)	19
Optional Elements	20
Recommended Optional Elements	20
Post (Publish) a CVE Record	22
Post the Test environment	23
Post to Production CVE.org environment	23

¹ This version of the document is from the “live” document (comments removed) and was retrieved 9 July, 2024 from https://docs.google.com/document/d/1c5EDddCErGHMsv_i-GjeGr-u7YDJ_HDu0TZXqyOFI0.

Update a CVE Record	24
Dispute a CVE Record	24
Reject a CVE ID or CVE Record	26
Reject a Reserved CVE ID	26
Reject a Published CVE Record	26
Publishing a Rejected CVE Record	28
List Reserved, Published, and Rejected CVE IDs	29
8 Advanced Topics	29
CPE	29
9 Additional Information	33
CVE and NVD	33
CVE Services Credential Security	34
CVE Services and Record Format Documentation	34

1 Overview

This document explains, step-by-step, how to use Vulnogram with CVE Services to manage users, CVE IDs, and CVE Records. [Vulnogram](#) is a tool for creating and editing CVE information in CVE JSON format, and for generating advisories. This guide is intended for CNAs who may operate at a comparatively smaller scale and who are not or using custom integration with CVE Services. Vulnogram is maintained by a CVE Program member ([chandanbn](#), thank you) and is not formally owned by the CVE Program.

NOTE: Please note that this document is a work-in-progress, and the authors welcome pertinent feedback and commentary. Issues with formatting and images will be resolved as this document is transitioned to a more final form. The authors apologize for any temporary inconveniences or accessibility issues.

Quick Start

See [QuickStart - Reserving, Populating, and Posting a CVE Record](#) for a shorter explanation of how to publish a CVE Record to the CVE List.

2 Terminology

This document uses terms defined in the [CVE Glossary](#).

The [CVE Services](#) web page uses the terms “Organizational Administrator” or “OA” to indicate a CVE Services user account with the administrator role. This document uses the terms “Administrator” or “Admin” (as used in Vulnogram) to mean “Organizational Administrator” or “OA.”

3 Becoming a CVE Numbering Authority (CNA)

An organization may apply to be a CNA [via the CVE Program website](#). Only CNAs can obtain production CVE Services accounts.

4 Getting CVE Services Credentials

Only active CNAs with a valid CVE Services User Account are eligible to use CVE Services in production. CNA organizations MUST have one or more Administrators and may have any number of individual user accounts.

Test Credentials

Separate credentials are required for the CVE Services test environment. These credentials may be provided during CNA onboarding and will be the first step in becoming familiar with CVE Services.

1. Contact your Root or Top-level Root
 - a. Root confirms CNA status
 - b. Root provides next steps
2. Follow your Root's or Top-level Root's instructions for obtaining one or more CVE Services Test credentials. CNA may be required to complete a form or application to acquire test credentials.

Production Credentials

Each CNA has one or more CVE Services Administrators that will be used to manage individual user accounts. These are the steps to follow when acquiring an initial Administrator account for CVE services. This account can be used to add additional CNA individual accounts later.

1. Contact your Root ([CISA ICS](#), [Google](#), [INCIBE](#), [JPCERT/CC](#), or [Red Hat](#)) or Top-level Root ([CISA](#) or [MITRE](#))
 - a. Root confirms CNA status
 - b. Root provides guidance on next steps
2. Follow your Root's or Top-level Root's instructions for obtaining CVE Services Administrator credentials. CNA may be required to complete a form or application to acquire credentials.
3. Save your new credentials securely; you may now use your CVE Services as an Administrator.

5 Vulnogram

Getting Started

Vulnogram is a JavaScript application that runs in your web browser. Vulnogram does not require a web server, but as used in these instructions, Vulnogram needs to communicate with CVE Services directly over the Internet.

Open the [Vulnogram](https://vulnogram.github.io) web app in your browser: <https://vulnogram.github.io>.

NOTE: As a browser JavaScript application, Vulnogram can exhibit issues related to web browser behavior, caching, network conditions, and other factors. For example, certain buttons may not respond when clicked or may be 'ghosted,' especially when switching between accounts. The usual website troubleshooting techniques apply: Try refreshing, clear browser settings for vulnogram.github.io, try a private window, or try a different web browser.

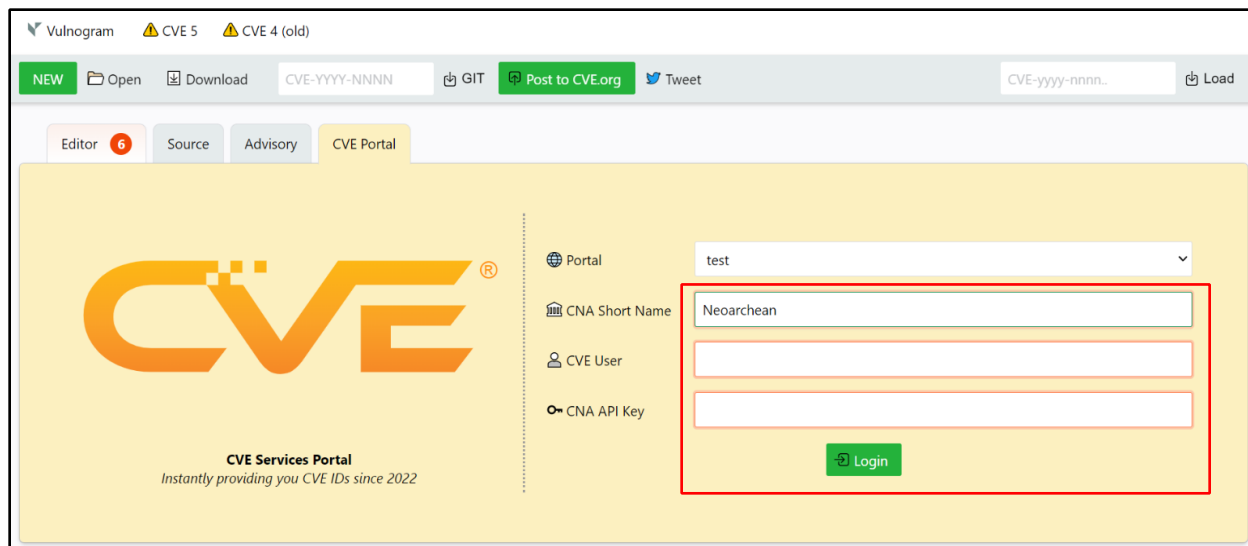
NOTE: In general terms and in our experience, Vulnogram works somewhat better with Google Chrome than Firefox, the two browsers we use most in testing. More specifically, we had issues with service workers using Firefox, but did not investigate in detail.

CVE Portal Tab

1. Navigate to [Vulnogram CVE Portal](#). From the Vulnogram Editor tab you can click on the yellow 'CVE Portal' tab.
2. Select either 'test' or 'production' portal.

WARNING: The 'production' portal handles live production CVE data. All CNAs should start within the test environment before attempting to use the production environment and live CVE data.

3. Enter your CNA Short Name, CVE User email address, and your CNA API Key (provided to you by the Root or TL-Root).



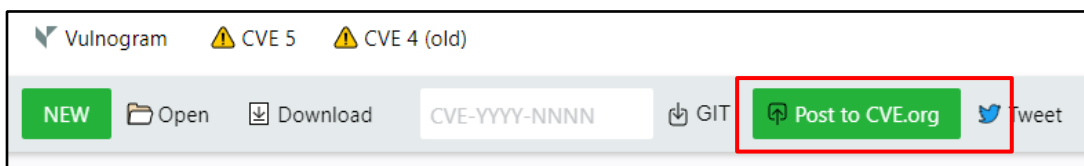
4. Click 'Login.'

WARNING: Depending on your browser state, your login to CVE Services may remain active. Confirm that you are logged in to the correct environment by examining the green button that reads either "Post to CVE.org" (production) or "Post to Test Portal" (test). Alternatively examine the "CVE Portal" tab, which will display which portal you are logged into.

Test Portal:



Live Production



Editor Tab

The [Editor](#) tab allows users to input CVE Record information, load existing CVE Records, and post CVE Records directly to CVE.org.

Source Tab

The [Source](#) tab allows users to directly view and edit a CVE Record's JSON. Changes made in the Source tab will be reflected in the Editor tab (and changes in the Editor tab will be reflected in the Source).

NOTE: Some users have reported bugs or issues when using or navigating to or from the Source Tab, including inserting characters that the user did not enter. Be sure to double-check your CVE Record information when using the Source Tab.

Preview Tab

The Preview tab displays a preview of the current CVE Record and summary of required information. The Preview tab allows users to download the current advisory as HTML or to send the Advisory via Email by clicking the 'Download' or 'Email' buttons, respectively.

Vulnogram CVE 5 CVE 4 (old)

NEW Open Download Post to Test Portal CVE-yyyy-nnnn... Load Edit

Editor 2 Source Preview CVE Portal

CVE-yyyy-nnnn

Published by Neorchain on 2024-02-29 (updated 2024-03-04)
In example product version 7.4, a component was vulnerable to XYZ if ABC.

Problem:

Product Status:

Product	Affected
Vendor Product	7.4
Default status is affected	

References

www.cisa.gov

Download Email

6 User Management

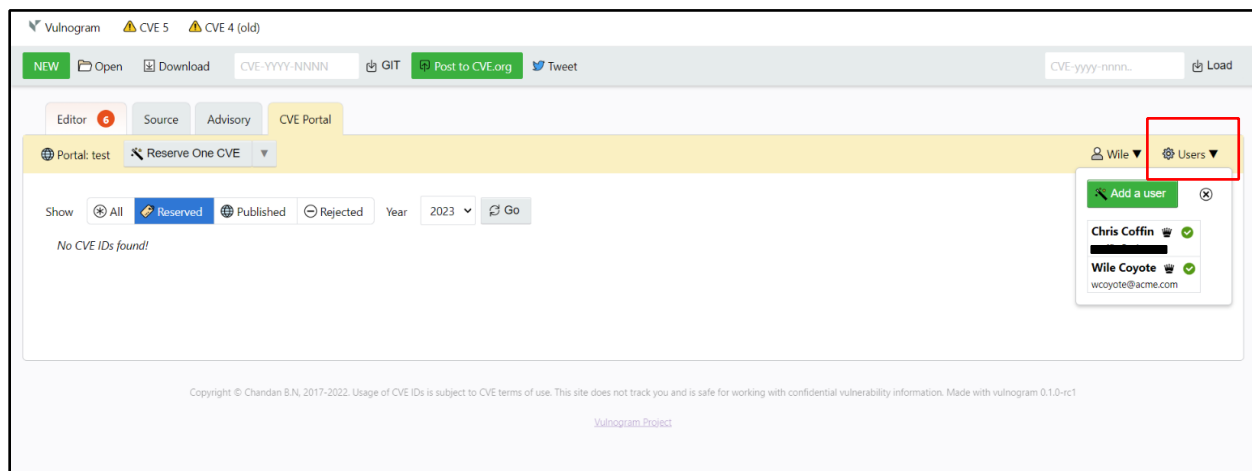
The following sections describe common tasks for managing users. To manage users, you must be logged into an account with Administrator privileges.

Create a User

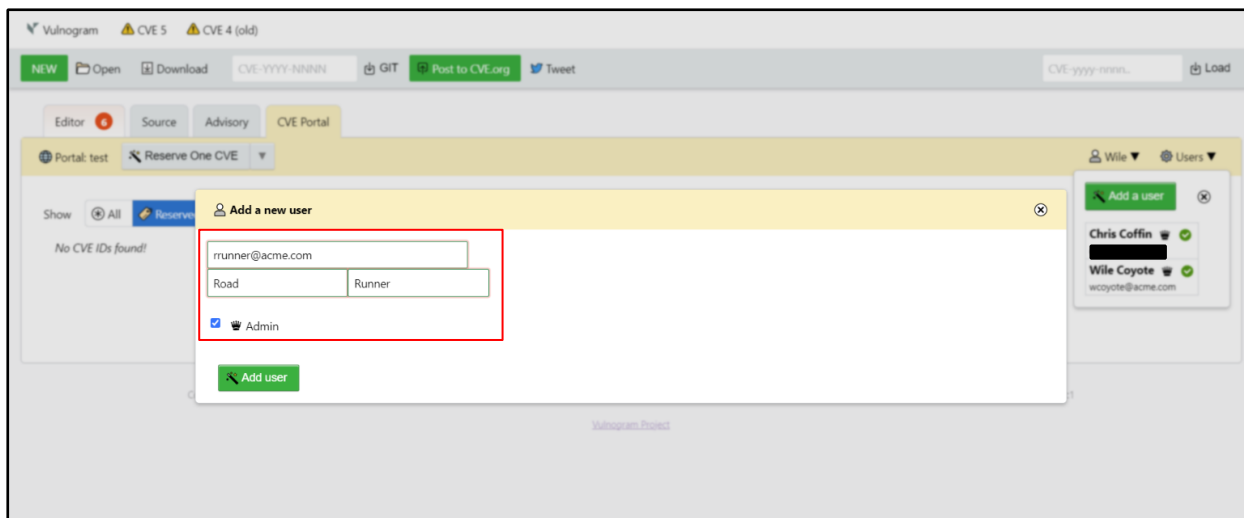
User accounts can be added and managed by an Administrator and do not require coordination with the Root.

WARNING: Due to a bug, newly-created users will **have Administrator privileges by default**. You must remove individuals' Administrator privileges manually *after* the user is successfully created. See [Manage Administrators](https://github.com/Vulnogram/Vulnogram/issues/162). Github issue: <https://github.com/Vulnogram/Vulnogram/issues/162>

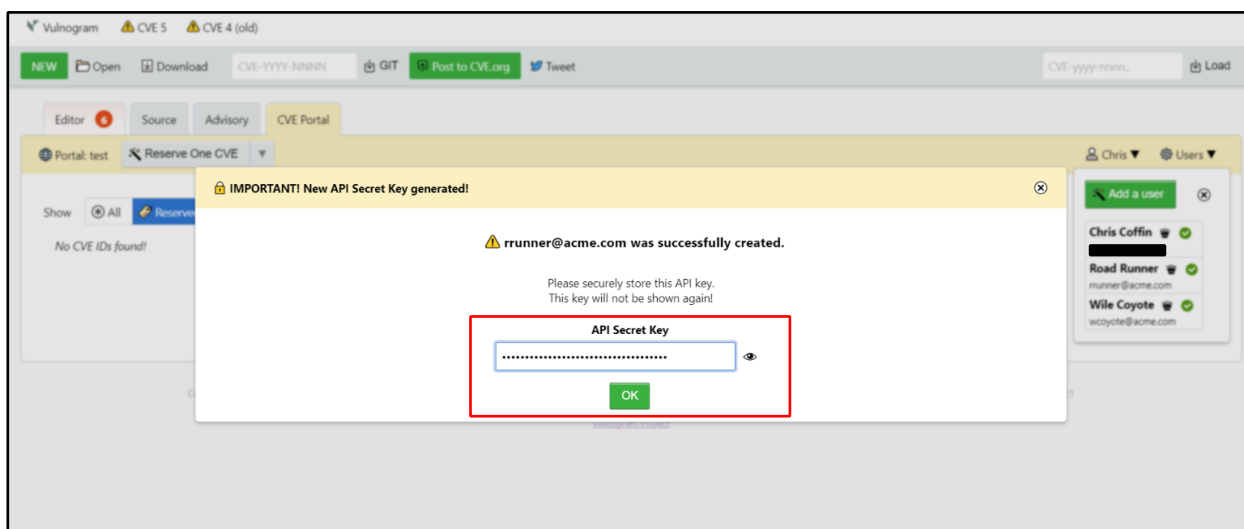
1. Login to Vulnogram with an existing Administrator account
2. Navigate to [Vulnogram CVE Portal](#)
3. Select the “Users” drop down on the far right of the interface



4. Select the “Add a user” button from the drop down
5. Enter the new username, First and Last names, and check the box next to ‘Admin’ if they will be an Administrator account



6. Click the “Add user” button when finished.
7. If successful, a new window is displayed with the new users API secret key. This key should be saved securely and will be needed for all future logins using the newly created user account.



Change User Information

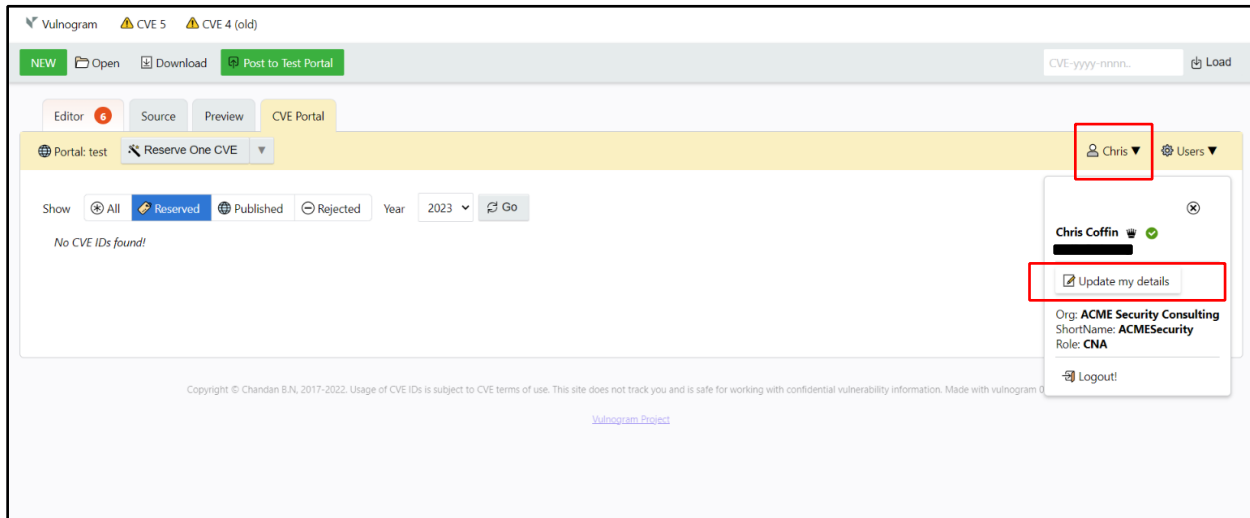
This section describes how to change the user login name (aka CVE User). Only Administrator accounts can change user login names.

User ID

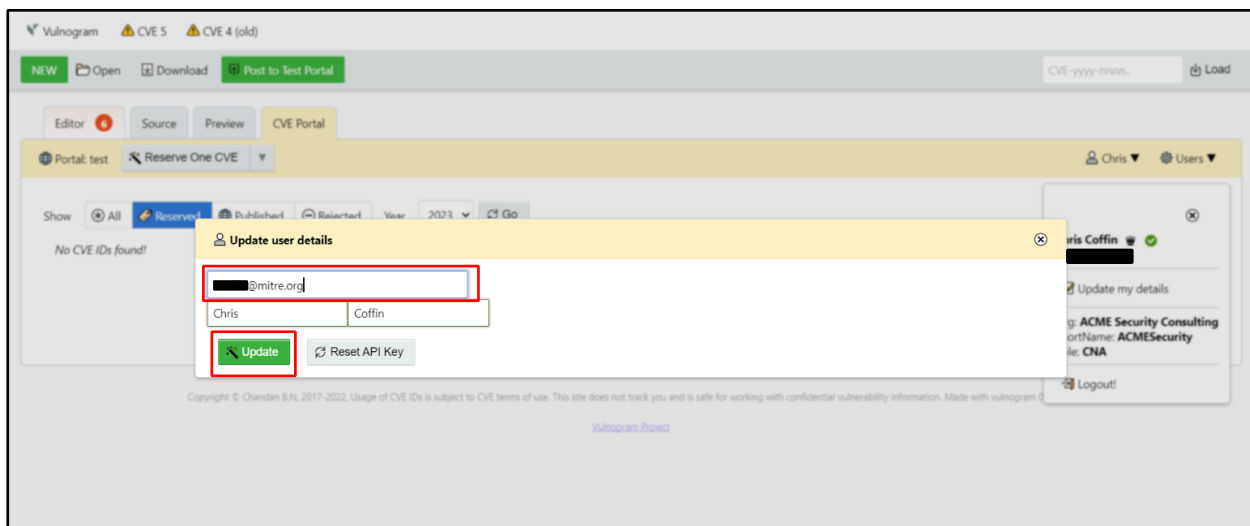
By convention User ID is usually an email address, but it can be any string.

1. Navigate to [Vulnogram CVE Portal](#).
2. Select the drop-down for the currently logged in user (top right of display)

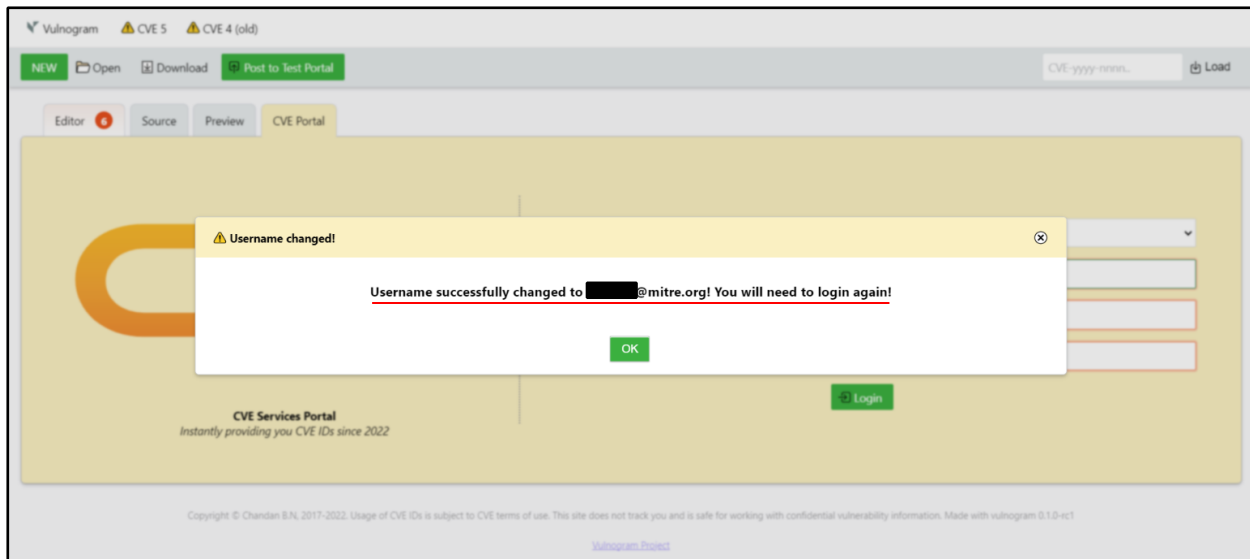
3. Select the “Update my details” button.
 - a. If the intent is to change a different user login name than the one currently logged in, select the Users drop-down and select the applicable user from the list. The latter option can also be used as an alternative to change the currently logged in user name. This requires an Administrator account.



4. Change the login user name (first box at the top of the window) and then select the Update button.



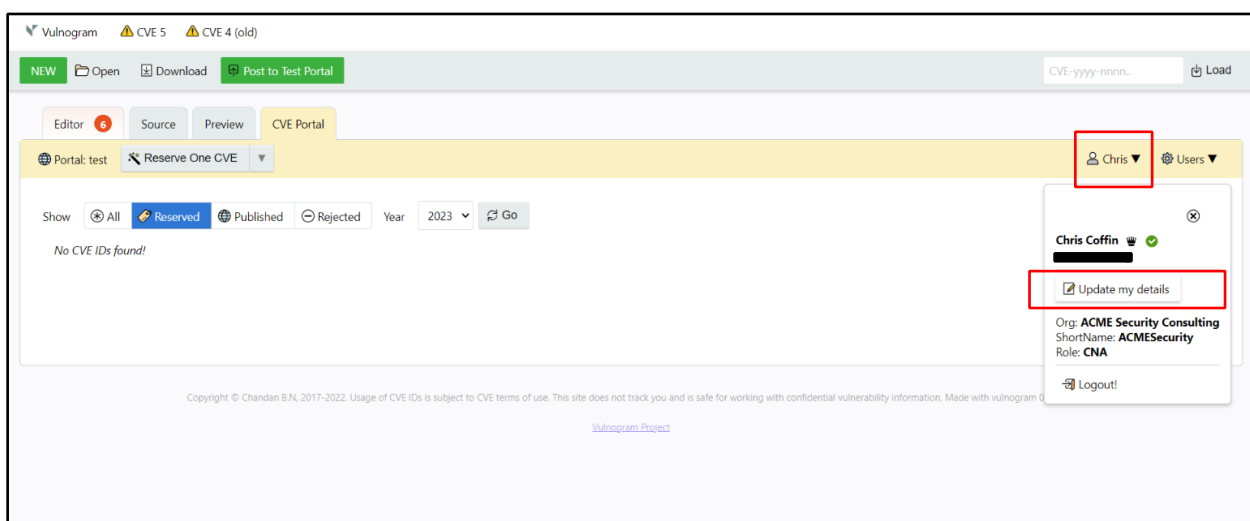
5. If the currently logged in user's name was changed in step 2, a notification window will be displayed letting the user know that they must login again because of the name change. Clicking OK will bring the user to the Portal login. If a different user's login name was changed in step 2, the user login name is updated and the UI is returned.



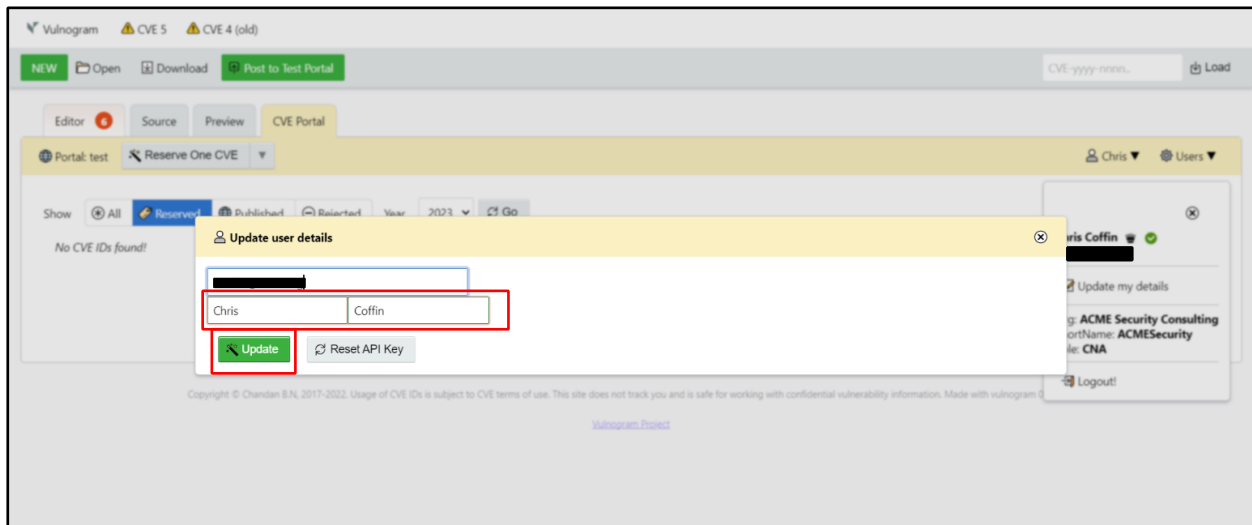
User Name

This section describes how to change a user's first and/or last name. Regular users can change their first and last name only, while Administrators can change the first and/or last name of any account under the CNA.

1. Navigate to [Vulnogram CVE Portal](#).
2. Select the drop-down for the currently logged in user (top right of display)
3. Select the "Update my details" button.
 - a. If the intent is to change a different user login name than the one currently logged in, select the Users drop-down and select the applicable user from the list. The latter option can also be used as an alternative to change the currently logged in user name. This requires an Administrator account.



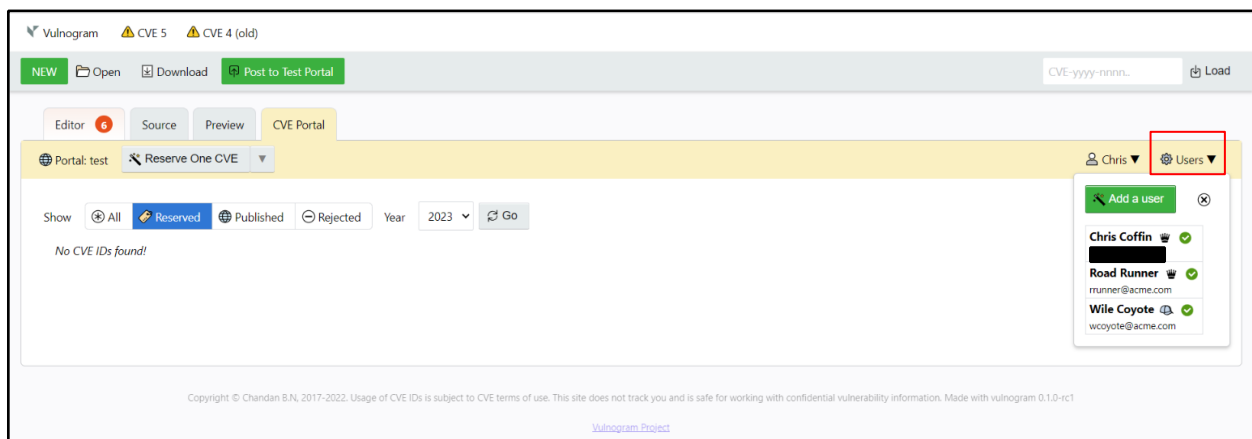
4. Change the user first and/or last name (second row of dialog boxes) and then select the Update button. The user's first and/or last name is updated immediately after selecting the Update button.



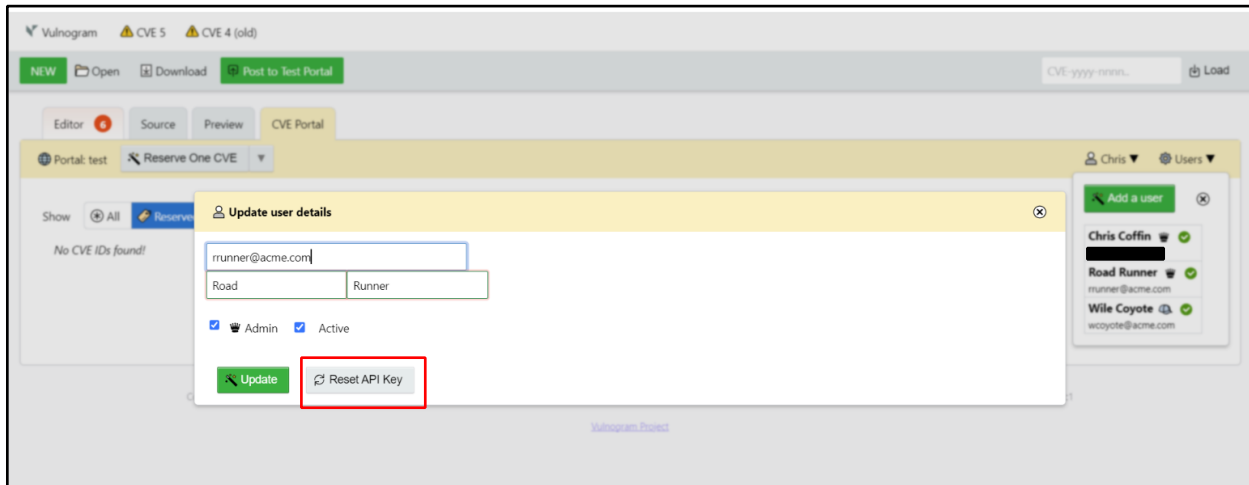
Reset API Key

This section describes how to reset the API key for a user. The API Key is essentially the user password. If an API Key has been lost for any CNA account, an Administrator under the CNA can login to the Vulnogram client, select the user in question, and reset the API Key (instructions below). If a CNA has misplaced their only Administrator account API Key, they will need to contact their Root or Top-Level Root to get their API Key reset. Note that if the Administrator user realizes that they have lost their API Key and are still logged in to the Vulnogram client, they can reset their own API Key using the steps below.

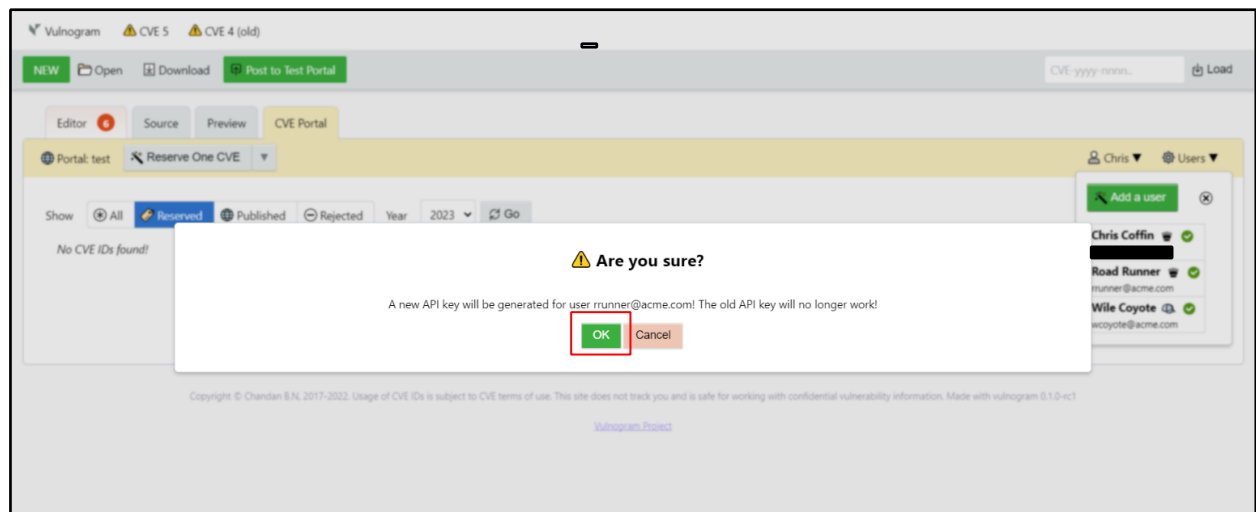
1. Navigate to [Vulnogram CVE Portal](#) and login as an Administrator.
2. Select the Users drop-down and choose the user who's API Key is to be reset.



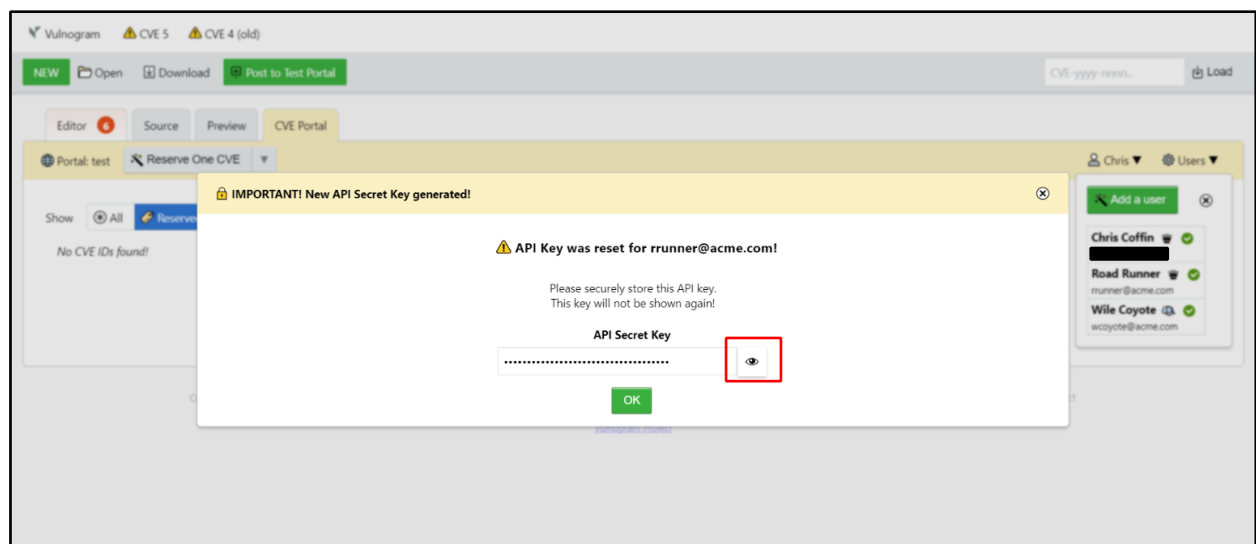
3. Select the “Reset API Key” button.



4. A notification window will appear to confirm the generation of a new API key for this user. Select OK.



5. The resulting window displays the new API key for the user. Selecting the 'eye' button to the right of the key will unhide the characters. This API key should be given to the user in question and they should save the API key for future portal logins.



Manage Administrators

This section describes how to change a Regular user to an Administrator and back. Administrator accounts have the ability to manage other users in addition to performing editing and submitting CVE content using the CVE services. Regular users cannot manage other users and are only allowed to edit and submit CVE content using CVE services. When an Administrator is logged into the Vulnogram client, they will see a Users drop-down on the top

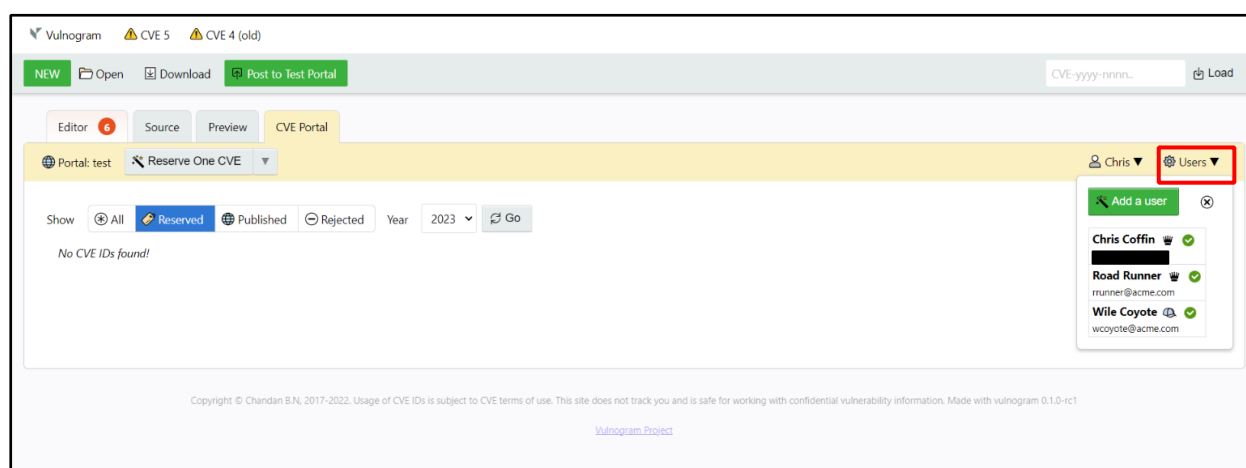
right of the interface. Selecting this drop-down will display all users defined under the CNA. A crown icon will be displayed for Administrators and a hat icon is displayed for Regular users.

The instructions below describe how to change a Regular user to an Administrator. The same instructions can be used to change an Administrator to a Regular user by changing the last step as noted below.

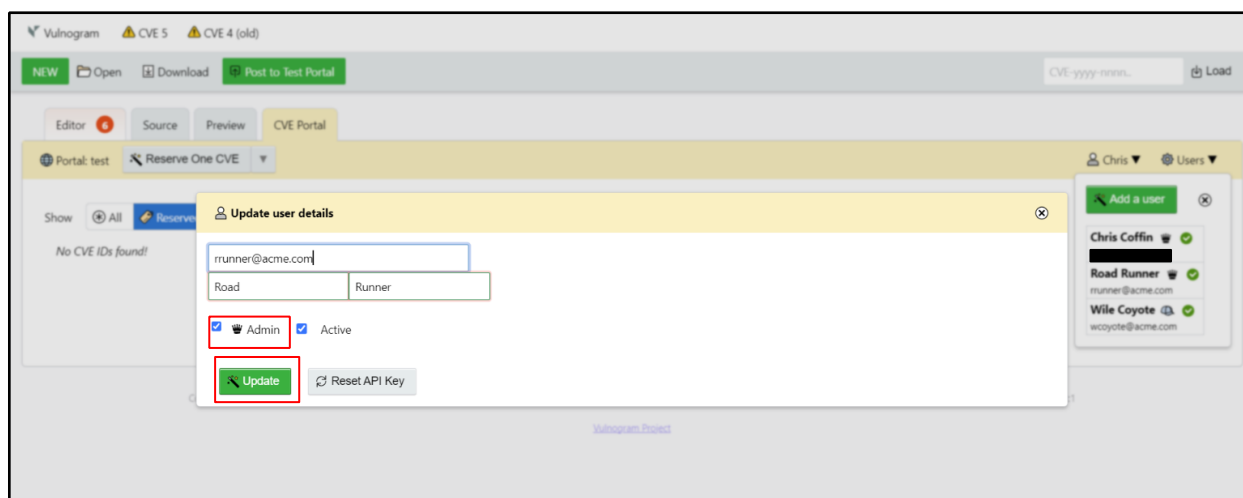


WARNING: ANY Administrator can grant or revoke the Administrator role within their organization. Any newly-created Administrator can revoke privileges from other accounts. It is possible for the last Administrator to remove the Administrator role from their account, leaving a CNA with no Administrator accounts.

1. Navigate to [Vulnogram CVE Portal](#) and login as an Administrator.
2. Select the Users drop-down and choose the Regular user who will be granted the “Admin” role.



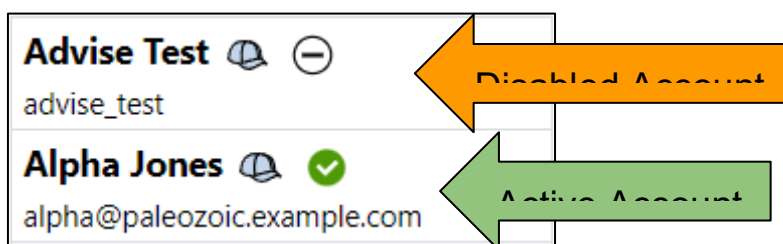
3. Put a check in the box to the left of the text “Admin” at the bottom of the Update user details window and select the Update button.



4. The user will now have the Admin role and can manage other user accounts. If the Admin role must later be removed from this or any other CNA account, the same steps can be followed except to remove the check in the box next to "Admin" in step 3.

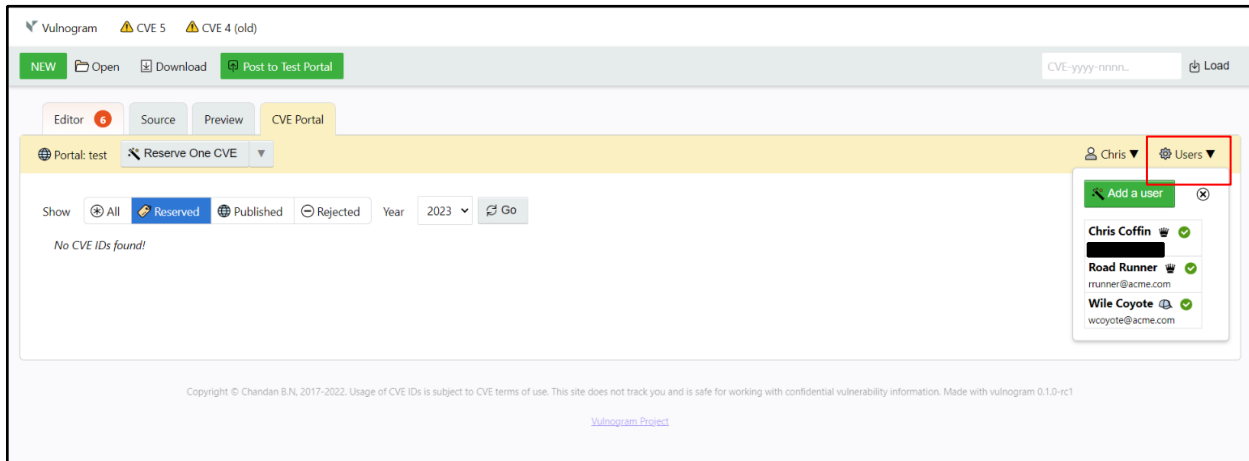
Disable and Enable Users

This section describes how to disable a user. Note that users cannot be deleted at this time. When viewing the Users list as an Admin in Vulnogram, Active user accounts have a green circle with white checkmark next to them, while disabled accounts have a black outlined circle with a black negative symbol.

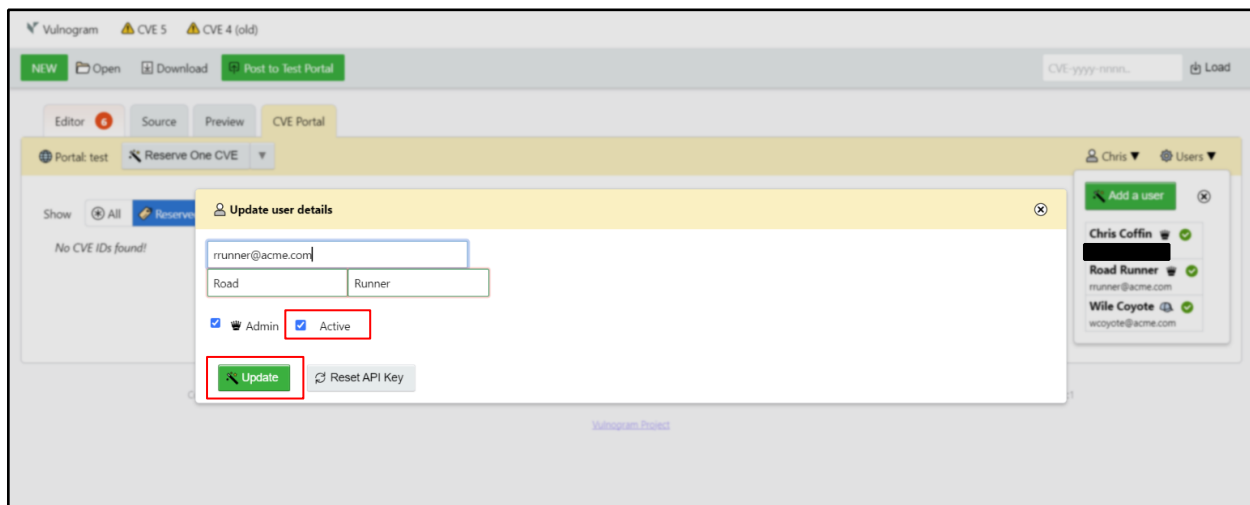


1. Navigate to [Vulnogram CVE Portal](#) and login as an Administrator.

2. Select the Users drop-down and choose the user who is to be disabled.



3. Uncheck the box to the left of the text “Active” at the bottom of the Update user details window and select the Update button.



4. The user will now be disabled/inactive. If this user or any other disabled user later needs to be reactivated, the same steps can be followed except to replace the check in the box next to “Active” in step 3.

7 CVE Record Management

QuickStart - Reserving, Populating, and Posting a CVE Record

The sections that follow include detailed guidance on how to perform various CVE record management tasks. However, a common use case for CNAs is to reserve, populate, and post a

single new CVE record all at the same time. The steps necessary to perform this operation are listed here, along with a reference to the more detailed sections that follow where appropriate.

1. Navigate to the [Vulnogram CVE Portal](#) tab and log in.
2. Click 'Reserve One CVE' (See "[Reserve a CVE ID](#)" section for more details).
3. The newly-reserved CVE ID will appear on the list of reserved CVE IDs, along with its requester and date of creation.
4. Click on the resulting new CVE Record ID that appears in the portal list. This will open the Vulnogram Editor tab with the CVE ID of the new CVE record.
5. Fill in the details of the CVE record within the Vulnogram Editor tab (See "[Populate \(Write\) a CVE Record](#)" section for more details).
6. When the CVE record is ready to be published, click the green button marked 'Post to CVE.org' (See "[Post \(Publish\) a CVE Record](#)" section for more details).

Reserve a CVE ID

1. Navigate to the [Vulnogram CVE Portal](#) tab and log in.
2. Click 'Reserve One CVE.'
 - a. Users may use the dropdown arrow to reserve multiple CVE IDs or to reserve one for the upcoming or previous year.
3. The newly-reserved CVE ID will appear on the list of reserved CVE IDs, along with its requester and date of creation.

- Clicking on a reserved CVE ID that you wish to populate will open a fresh Editor tab with empty fields.

Vulnogram ⚠ CVE 5 ⚠ CVE 4 (old)

NEW Open Download CVE-YYYY-NNNN GIT Post to CVE.org Tweet

Editor Source Advisory **CVE Portal**

Portal: test **Reserve One CVE** ▼

Got CVE-2023-1631

Show All **Reserved** Published Rejected Year 2023 Go

ID	Requester	Created ▼	Modified
CVE-2023-1631	Redacted	2023-11-17 12:09	
CVE-2023-21408		2023-11-09	
CVE-2023-21151		2023-10-04	
CVE-2023-21150		2023-10-04	
CVE-2023-21149		2023-10-04	
CVE-2023-21148		2023-10-04	
CVE-2023-21129		2023-08-10	
CVE-2023-21128		2023-08-09	

Populate (Write) a CVE Record

A CVE Record requires certain information elements. Vulnogram highlights these elements in red and enforces the requirements. A CVE Record that is missing any of the required elements cannot be submitted by Vulnogram and will not be accepted by CVE Services. The [CVE Record Format](#) defines the elements.

CVE Record information should be filled out using Vulnogram's [Editor](#) tab.

The Vulnogram CVE Record Editor tab looks like this:

Vulnogram CVE 5 CVE 4 (old)

NEW Open Download CVE-YYYY-NNNN GIT Post to CVE.org Tweet CVE-yyyy-nnnn Load

Editor 6 Source Advisory 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 mm/dd/yyyy --:--:-- CDT

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)

Affected?	Version (or start of a range)	Version (range)	Version (range)	status changes (patches, split ranges)	versionType
<input checked="" type="checkbox"/>	eg., 1.2.0; 0 means no lower limits	eg., 1.2.0, 1.2.*	eg., 1.2.7, 1.2.*	+ item	eg., patch 10, 1.2.1

+ Version

Required Elements

The CVE Record Format requires the following elements.

CVE ID

Each CVE Record will have a unique CVE ID with the format CVE-YYYY-NNNN. Reserving a CVE ID will generate a new ID number. Clicking the 'cve.org' button to the right of the CVE ID field will open the corresponding CVE entry on [CVE.org](https://cve.org), if it already exists.

Editor 6 Source Advisory CVE Portal

CVE ID * CVE-yyyy-nnnn cve.org Enter CVE-yyyy-nnnn format.

Affected Products

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)

Affected?	Version (or start of a range)	< Version (range)	<= Version (range)	status changes (patches, split ranges)	versionType
<div> y n ⓘ ?</div>	eg., 1.2.0; 0 means no lower limits	eg., 1.2.8, 1.2.*	eg., 1.2.7, 1.2.*	+ item	eg., patch

+ Version

Default status (for versions not specified above)

y n ⓘ ?

- (Vendor or project AND Product name)
- OR
- (Package collection URL AND Package name)
- Platforms
 - Versions (exact versions or ranges)

The Affected Products section requires users to enter a combination of identifiers to distinguish each vulnerability. Users **MUST** enter both the Product's name *and* Vendor, or for a vulnerable package both the Package name *and* Package collection URL. Users should also specify the affected Platforms when applicable.

Enter a vendor and product OR a package and a collection

Vendor or project ⓘ

eg., Linux

Product name ⓘ

eg., Linux Kernel

Package collection URL ⓘ

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

Package name ⓘ

eg., kernel

The Versions section identifies which version(s) of a product are affected by the vulnerability. Users can enter either a single version or specify a range of versions. If only one version is affected, do not enter a range. Users must enter at least one affected version, but the Versions section also allows users to specify versions that are **not affected**. By default, versions not

specified in this section are marked as **not affected**, but users can select **not affected** or **unknown**. Users should be as specific as possible in this section.

NOTE: Additional fields under the Affected Products section (e.g., Source repository, Program routines) are NOT required for a complete CVE Record and are not covered in this section.

CVE Description

CNAs must enter a prose description of the vulnerability. While less important now that CVE JSON encodes more information about the vulnerability, a concise and accurate description is still very useful to CVE consumers. CNAs may elect to Auto Generate the description from data elsewhere in the same Vulnogram entry. [CVE Program Key Details Phrasing](#) provides further

Versions (exact versions or ranges)			
Affected?	Version (or start of a range)	< Version (range)	<= Version (range)
y n ?	eg., 1.2.0; 0 means no lower limits	eg., 1.2.8, 1.2.*	eg., 1.2.7, 1.2.*

+ Version

Default status (for versions not specified above) y n ?

guidance on writing a helpful description.

NOTE: Vulnogram's automatically-provided description template (see screenshot below) should serve as a suggestion, not a requirement. Users are free to adjust the syntax of their description as necessary to convey information about the CVE in a concise and accurate manner.

CVE Description

Auto Generate *

B *I* U **P** **H** **H** **H** *I*_x

[PROBLEMTYPE] in [COMPONENT] in [VENDOR] [PRODUCT] [VERSION] on [PLATFORMS] allows [ATTACKER] to [IMPACT] via [VECTOR]

Reference(s)

Users **MUST** include at least one reference to a publicly-available source supporting the data contained elsewhere in the CVE Record. It may be necessary to include more than one reference. Tags may be assigned to references to quickly describe them.

References *

URL	tags	
https://example.org	vendor-advisory ×	×
https://		×

Enter a valid URL.

+ Reference

Optional Elements

The CVE Record Format allows optional elements. Some of these are selected and included by default in Vulnogram. You will need to decide which optional elements to use and may have to remove optional elements included by Vulnogram. If you choose not to use an optional element, make sure to remove it by clicking the red “X” icon usually in the upper right of the element.

NOTE: While CVSS, CWE, and CPE information are not strictly required in order to post a CVE record, doing so provides the downstream CVE consumers with more actionable information that can be useful for many vulnerability management activities. Other third-parties may add different CVSS, CWE, and CPE information at a later time in their own data collections, but the CNA-provided information within the CVE record is widely considered to be authoritative.

Recommended Optional Elements

Public at ([datePublic](#))

“Public at” records the date that the vulnerability (not the CVE Record) was Publicly Disclosed.

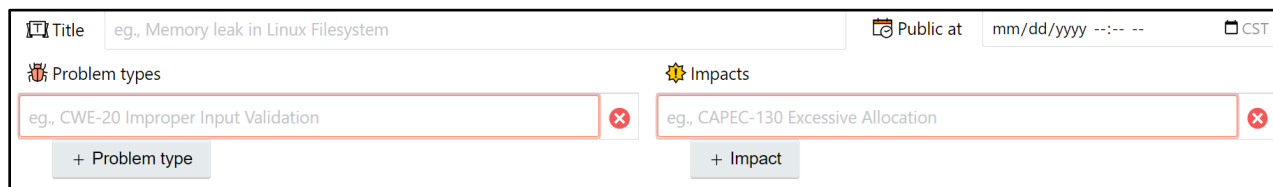
WARNING: “Public at” (datePublic) is informative only and does NOT schedule, postpone, or in any way affect the actual publication of the CVE Record.

Problem types ([problemTypes](#))

At least one “Problem type” should be provided and should use [CWE](#). Select a problem type from the drop down list or type a problem type string. However, the preferred method is to enter a CWE ID to capture the root cause weakness type as defined by the CWE Program. A default list of CWEs are provided in the drop-down menu to choose from, but the list is not currently complete. If the correct CWE is not included in the drop-down menu list, the CWE ID can be entered directly into the problem types field.

Impacts ([impacts](#))

This element can use [CAPEC](#). “Impacts” is included by default but is not widely used. Select an impact from the drop down list, type an impact string, or click the red “X” icon to delete the element entirely (see screenshot below).



The screenshot shows a form with the following fields and controls:

- Title:** eg., Memory leak in Linux Filesystem
- Public at:** mm/dd/yyyy --:-- --
- CST:** [icon]
- Problem types:** A text input field containing "eg., CWE-20 Improper Input Validation" with a red "X" delete icon to its right. Below the field is a "+ Problem type" button.
- Impacts:** A text input field containing "eg., CAPEC-130 Excessive Allocation" with a red "X" delete icon to its right. Below the field is a "+ Impact" button.

CVSS 4.0 metrics

This element provides options for CVSS 4.0 Base and Supplemental metrics. A CVSS 4.0 Base metric is included by default and set to maximum values, resulting in a 10.0 Base score. Either modify the CVSS vectors appropriately or click the red “X” icon to delete the element entirely (see screenshot below).

Vulnogram CVE 5.1(beta) CVSS 4.0 CVE 5 (Current) CVE 4 (old)

NEW Open Download Post to Test Portal CVE-yyyy-nmm... Load

Rating Metric 1 - CVSS CVSS 4.0 CVSS 3.1 (Obsolete) CVSS 2 (Obsolete) SSVCv2.0 Other

Scoring scenarios *

GENERAL

+ Scenario

Common Vulnerability Scoring System (CVSS) 4.0 *

Attack Vector Physical Local Adjacent Network

Attack Complexity High Low

Attack Requirements Present None

Privileges Required High Low None

User Interaction Active Passive None

Product Confidentiality None Low High

Product Integrity None Low High

Product Availability None Low High

Safety Impact Not defined Negligible Present

Automatable attack Not defined No Yes

Recovery Not defined Automatic User Irrecoverable

Value Density Not defined Diffuse Concentrated

Vulnerability Response Effort Not defined Low Moderate High

Urgency Not defined Informational Reduced Moderate Hightest

Base Severity Score (TBD) Vector Open in CVSS Calculator

CRITICAL 10 CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:H/SH/SA:H

CVSS 3.1 metric ([metrics](#), [cvssV3_1](#))

This element provides a [CVSS 3.1 Base Metric](#). A CVSS 3.1 metric is included by default and set to maximum values, resulting in a 10.0 Base score. Either modify the CVSS vectors appropriately or click the red “X” icon to delete the element entirely (see screenshot below).

Rating Metric 1 - CVSS CVSS 3.1 CVSS 2 (Obsolete) SSVC Other

Scoring scenarios *

GENERAL

+ Scenario

Common Vulnerability Scoring System (CVSS) 3.1 *

Attack Vector Physical Local Adjacent Network

Attack Complexity High Low

Privileges Required High Low None

User Interaction Required None

Scope Unchanged Changed

Confidentiality None Low High

Integrity None Low High

Availability None Low High

Base Severity Score Vector Open in CVSS Calculator

CRITICAL 10.0 CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

Additional **optional** fields can be found at the bottom of the Vulnogram Editor tab and are not included by default.

- Required Configuration for Exposure
- Workaround
- Solution
- Exploit Status
- Timeline

- Credits
- Source

Required Configuration for Exposure (optional)

+ Config

Workaround (optional)

+ Workaround

Solution (optional)

+ Solution

Exploit Status (optional)

+ Exploit Status

Timeline (optional)

+ Event

Credits (optional)

+ Credit

CVE entry is sourced from

Defects

Source of vulnerability discovery

☐ internal
 ☐ external
 ☐ during use
 ☐ upstream
 ☒ undefined

Tags

- Tags

Post (Publish) a CVE Record

WARNING: Clicking 'Post to CVE.org' in Vulnogram will immediately publish the current CVE Record, assuming the Record is valid. Be careful not to accidentally publish CVE Records, especially when working vulnerabilities that are not yet meant to be Publicly Disclosed. To avoid accidentally publishing, you can intentionally use an invalid CVE ID, for example, "CVE-1999-1234-donotpublishyet." Vulnogram will *not* post a CVE Record with an invalid CVE ID. A Vulnogram [issue](#) has been filed requesting a confirmation dialog.

Post the Test environment

Remember to use the test environment when publishing your first few test records. You can verify that you are using the Test portal by viewing the Green “Post to...” button at the top of the Vulnogram window. The button will read “Post to Test Portal” for the Test environment, and “Post to CVE.org” for the production environment.

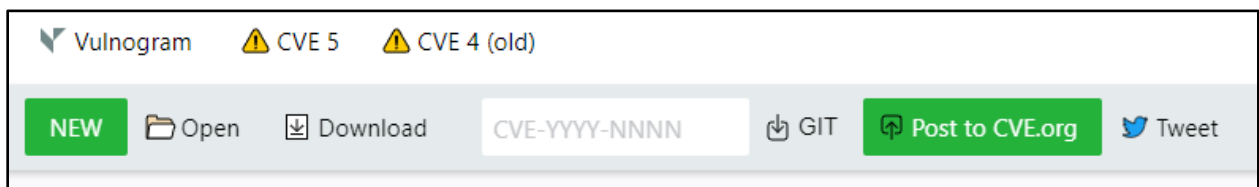
Test Portal:



To view your test records on the CVE test portal website, visit <https://test.cve.org> and enter your CVE ID.

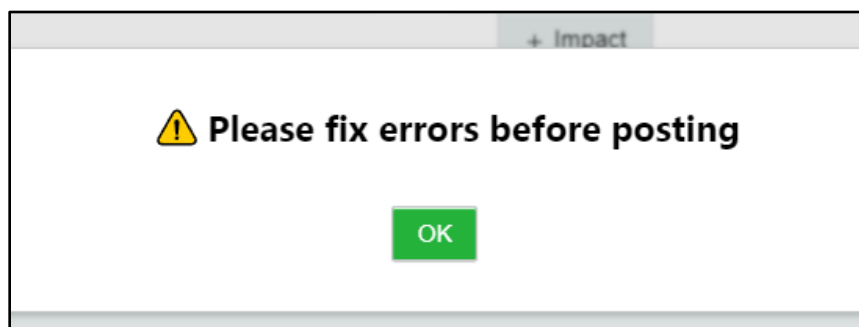
Post to Production CVE.org environment

To submit a completed CVE Record via Vulnogram, click the green button marked ‘Post to CVE.org.’



Users MUST fill all required elements before posting a CVE Record. A hyperlinked message will be displayed at the top of the Vulnogram window when a record has been posted successfully.

The message notes that the newly posted CVE record will be available within 15 minutes. If any required fields are unfilled the user will receive the following error message:

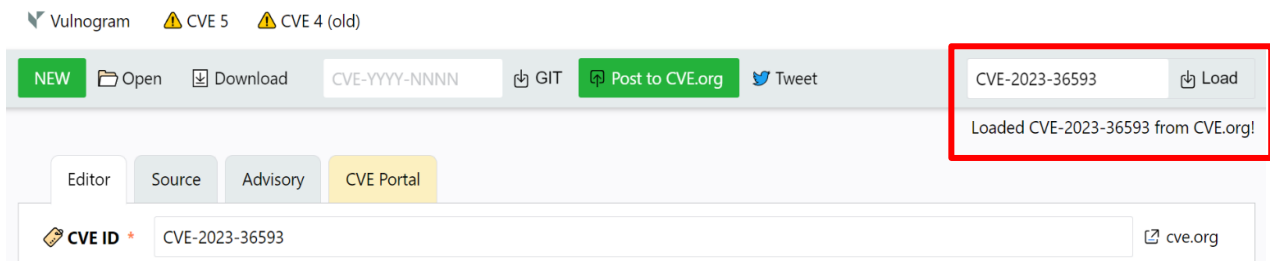


WARNING: Successfully posting a test CVE record to the Test portal results in a successful message that has the **wrong hyperlink**. The hyperlink points to the production CVE web site with the newly created Test CVE Record ID. This will result in the user seeing a different live CVE record or a blank record. To view the newly created Test CVE record, use <https://test.cve.org/cvarecord?id=CVE-1900-1234>, and replace CVE-1900-1234 with the intended CVE record ID. (See <https://github.com/Vulnogram/Vulnogram/issues/200>)

Update a CVE Record

WARNING: Posting to the CVE Services overwrites the entire CVE Record with the new content. Take care to load the current CVE Record content from the CVE Services before making updates.

1. While logged into the CVE Portal, enter the CVE ID of the Record you wish to update in the field at the top right of the screen.
2. Click 'Load.' The editor will populate with the existing CVE Record information.
 - a. Users should choose the 'Load' function to retrieve up-to-date CVE Records from CVE.org, rather than selecting 'Open' to edit a locally-saved JSON CVE Record.
3. Make any necessary additions or changes to the CVE Record.
4. Click the green box at the top of the screen marked 'Post to CVE.org.'



Dispute a CVE Record

Per the [CVE Program Policy and Procedure for Disputing a CVE Record](#), it may be necessary to mark a CVE Record as Disputed. To mark a published CVE Record as Disputed using Vulnogram, users must load, edit, and republish the CVE Record.

1. While logged into CVE Services, enter the published or reserved CVE ID of the Record you wish to mark as Disputed in the field at the top right of the screen.
2. Click 'Load.' The editor will populate with the existing CVE Record information.
 - a. Users should choose the 'Load' function to retrieve up-to-date CVE Records from CVE.org, rather than selecting 'Open' to edit a locally-saved JSON CVE Record.

3. Scroll down to the bottom of the Vulnogram client and find the “Tags” field, under the Metrics section.
4. Click in the “Tags” field to show the suggested options “unsupported-when-assigned,” “exclusively-hosted-service,” and “disputed.” **Select “disputed.”**

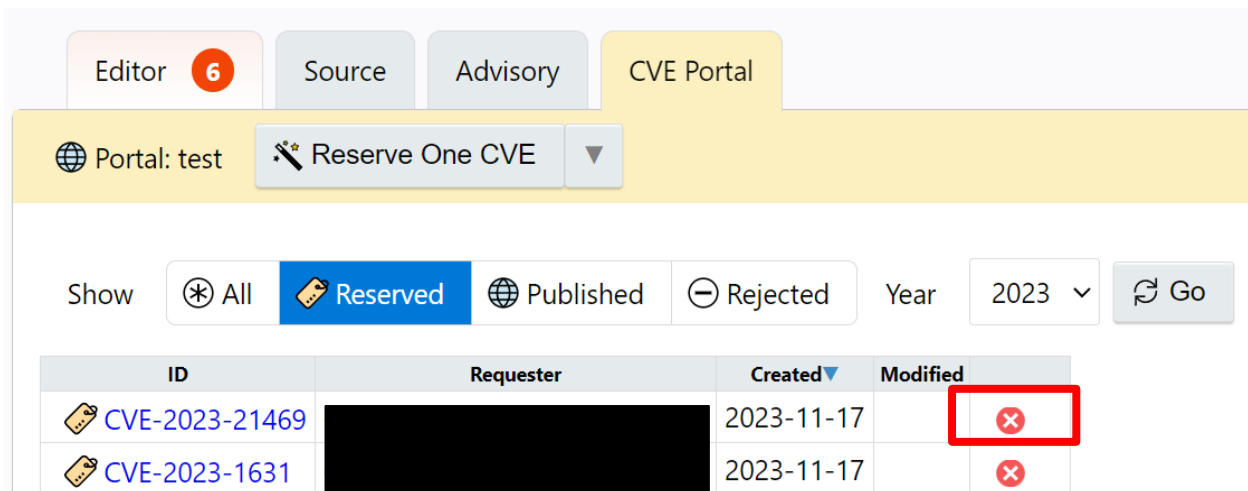
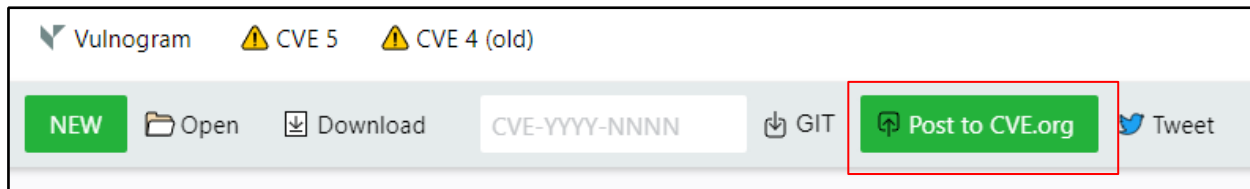
The screenshot shows the Vulnogram client interface. At the top, there's a 'Tags' section with a red box around it. Inside this section, there are three buttons: 'disputed', 'unsupported-when-assigned', and 'exclusively-hosted-service'. A red arrow points to the 'disputed' button. Below this, there's a 'Metrics' section with various fields like 'Credits (optional)', 'CVE entry is sourced from', 'Defects', 'Source of vulnerability discovery', and 'Advisory ID'. The 'Tags' field is highlighted with a red box, and the 'disputed' button is also highlighted with a red box. At the bottom, there's a green button labeled 'Post to CVE.org'.

5. Users should provide an explanation as to why the CVE Record is Disputed. Add text to the CVE Description to indicate the reason for Dispute.
6. Click the green box marked “Post to CVE.org” to update the CVE Record publicly.

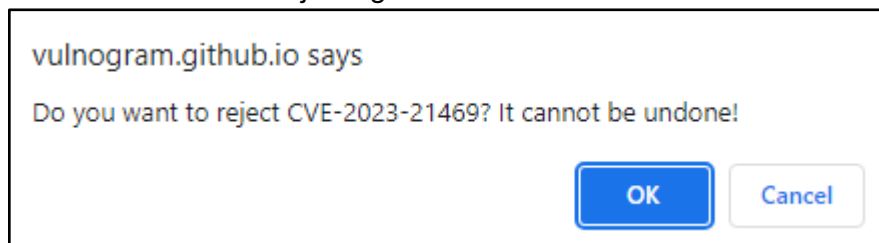
The screenshot shows the 'CVE Description' field. At the top, there's a green button labeled 'Auto Generate'. Below it, there's a text area with a red box around the text: "Example Software from Example Supplier prior to 1.0.3 has a vulnerability, using cvelib, this is CVE-2023-0216, with another update, using --cve-json-file cvelib-howto.21160. NOTE: the Supplier does not consider this issue to be a vulnerability."

Reject a CVE ID or CVE Record

Reject a Reserved CVE ID



1. While logged into the CVE Portal, navigate to your list of reserved CVE IDs.
2. To the right of each CVE ID, you will see a red 'X' icon. Click the red 'X' to reject a CVE ID.
 - a. Your browser will provide a warning that rejecting a CVE ID cannot be undone. Click 'OK' to finalize rejecting the CVE ID.

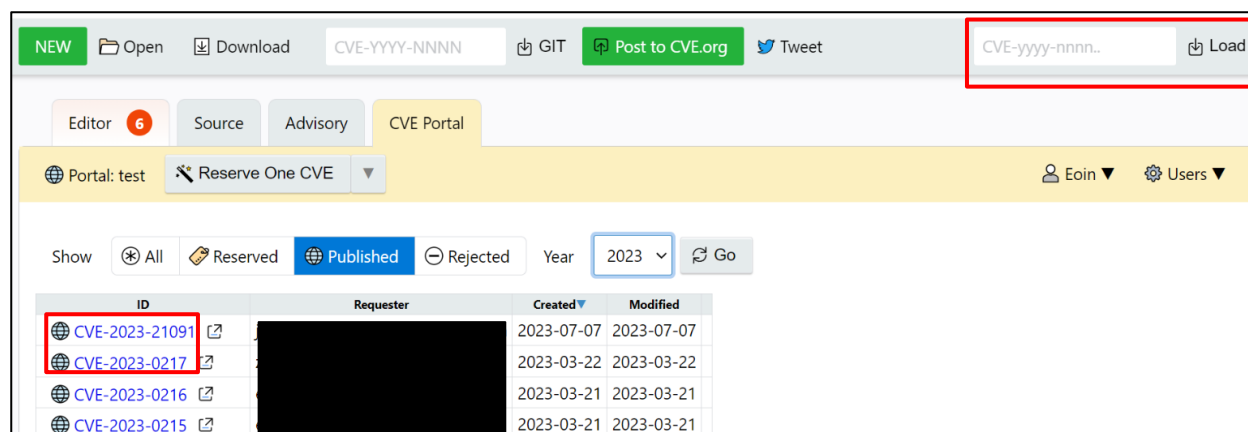


NOTE: It is not possible to “re-publish” or “un-reject a reserved CVE ID that has been rejected and was not published as a CVE Record. It is possible to publish a previously published, but now rejected, CVE Record (See [Publishing a Rejected CVE Record](#)).

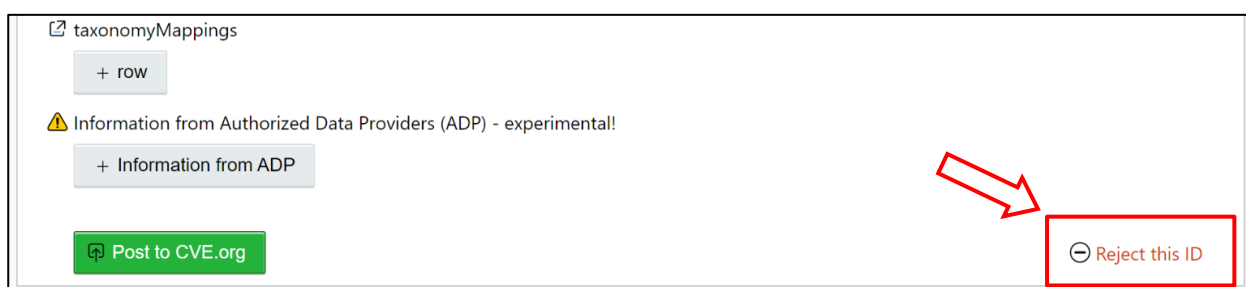
Reject a Published CVE Record

1. While logged into Vulnogram, navigate to the CVE Portal tab and your list of published CVE Records and find the Record you wish to reject.

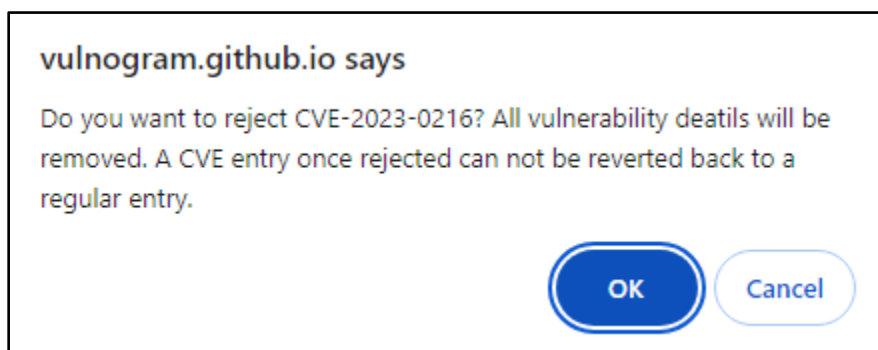
2. Click on the CVE ID to load the Record in the editor, or enter the CVE ID in the field at the top right of your screen and click 'Load.'



3. From the Editor tab, scroll down to the bottom right of the screen and click the button marked 'Reject this ID.'



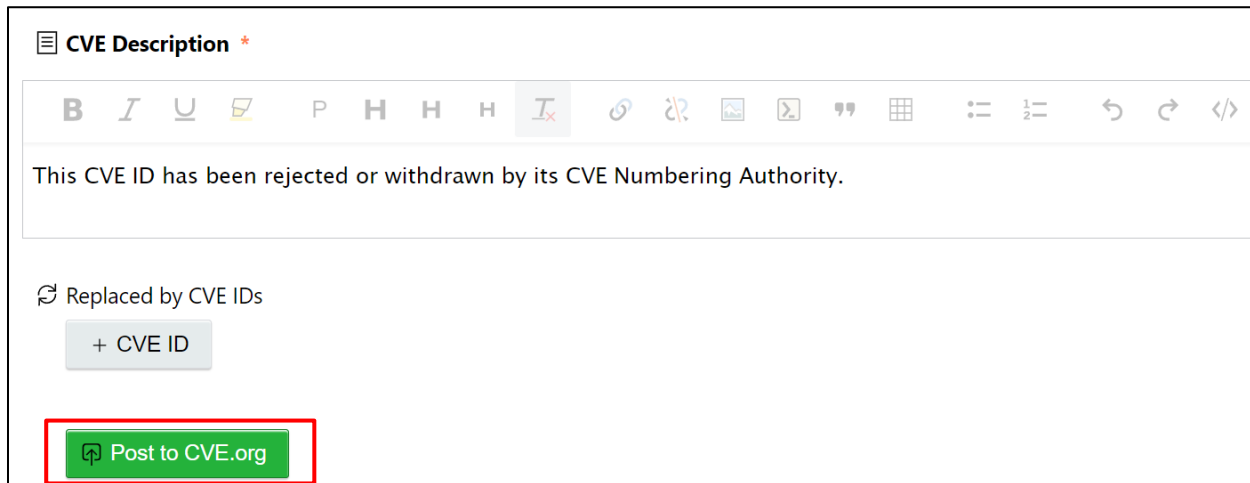
- a. Your browser will provide a warning that rejecting a published CVE Record cannot be undone.














Click 'OK' to finalize rejecting the CVE Record.

4. The CVE Description element will automatically update to reflect that the CVE ID has been rejected. You should add a brief reason for the rejection, for example, the Description for [CVE-2024-1087](#) states that "This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is a duplicate of CVE-2024-1085."

5. Click the green button marked “Post to CVE.org.” CVE services will now reflect that the Record has been rejected.



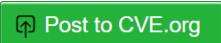
CVE Description *

B I U **P H H H** **I**           

This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.

↻ Replaced by CVE IDs

+ CVE ID

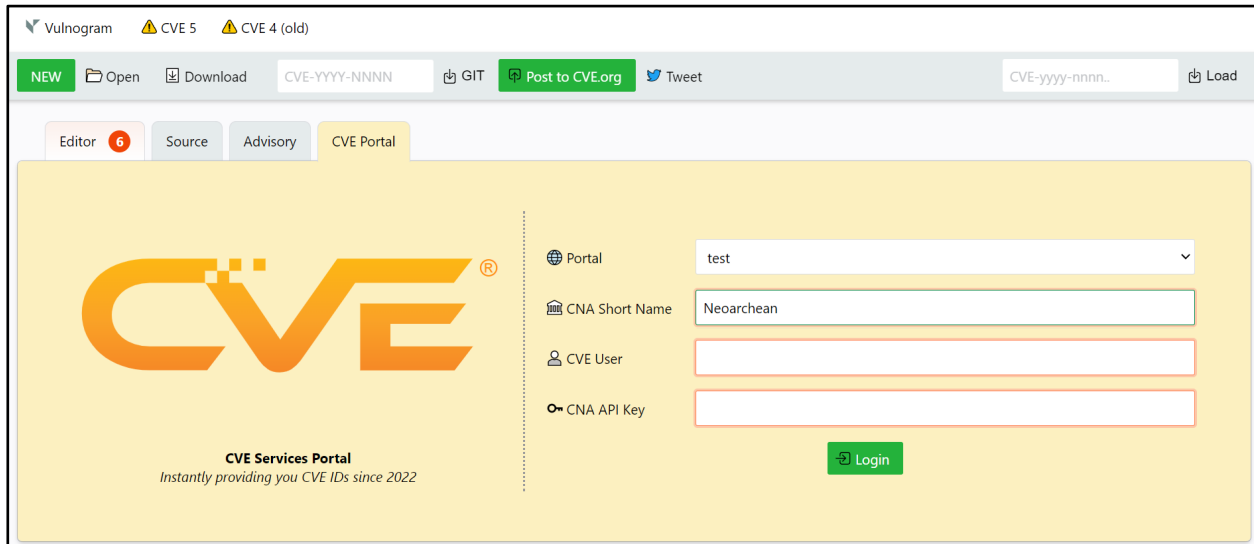
 Post to CVE.org

Publishing a Rejected CVE Record

To publish a previously rejected CVE Record:

1. Click the green button marked “NEW.”
2. Enter the CVE ID of the rejected CVE Record that you wish to re-publish in the “CVE ID” field.
 - a. Do NOT load the CVE Record via the “Load” box or by clicking on a CVE ID from the list of rejected CVE IDs.
2. Follow the steps to populate the CVE Record in [Posting a CVE Record](#) using the previously rejected CVE ID.
 - a. If you have a local copy of the JSON, you can click the ‘Open’ button and select the appropriate file.
3. Click the green button marked “Post to CVE.org.” CVE services will reflect your changes.

List Reserved, Published, and Rejected CVE IDs



The screenshot shows the Vulnogram CVE Services Portal. At the top, there's a navigation bar with 'NEW', 'Open', 'Download', a search bar containing 'CVE-YYYY-NNNN', 'GIT', 'Post to CVE.org', 'Tweet', and another search bar with 'CVE-yyyy-nnnn...' and a 'Load' button. Below this is a tabbed interface with 'Editor' (6), 'Source', 'Advisory', and 'CVE Portal' (selected). The main content area has a large orange 'CVE' logo on the left and a login form on the right. The login form includes a 'Portal' dropdown menu (set to 'test'), a 'CNA Short Name' text field (containing 'Neorarchean'), a 'CVE User' text field, and a 'CNA API Key' text field. A green 'Login' button is at the bottom right of the form. Below the logo, it says 'CVE Services Portal' and 'Instantly providing you CVE IDs since 2022'.

1. Navigate to the [CVE Portal](#) on Vulnogram and log in.
2. Select “Reserved,” “Published,” or “Rejected” tabs to view all of the corresponding CVE IDs from your organization.
 - a. Note: while logged into the Test or Production CVE Portal, the Reserved, Published, and Rejected tabs will only show CVE IDs that were Reserved/Published/Rejected via the currently-selected CVE Portal.
3. Users can select which year’s CVE IDs to display, and can sort by ID number, Requester, Date of Creation, or Date Last Modified.

8 Advanced Topics

CPE

Common Platform Enumeration ([CPE](#)) is a way to identify software components, including products and packages. While the CVE Record Format supports CPE to identify [Affected Products](#), the Vulnogram user interface does not currently support CPE. It is possible to manually edit JSON source to add CPE information, however doing so is not a reliable or scalable process. CNAs who choose to use CPE should carefully develop and maintain CPE information and integrate with the official NVD [CPE Dictionary](#). With this in mind, the following steps explain how to add CPE information to CVE records using Vulnogram.

1. Create the CVE record within Vulnogram in the standard way as described in the previous sections of this document

- When the CVE record is near completion and before posting the record to the test or production environments, open the Source tab of the Vulnogram display. The source tab shows and allows editing of the raw JSON of the CVE record as it's currently defined.

Vulnogram ⚠ CVE 5 ⚠ CVE 4 (old)

NEW Open Download Post to CVE.org

Editor Source Preview CVE Portal

```
1 {
2   "dataType": "CVE_RECORD",
3   "dataVersion": "5.0",
4   "cveMetadata": {
5     "cveId": "CVE-2024-0429",
6     "assignerOrgId": "00000000-0000-4000-9000-000000000000",
7     "requesterUserId": "00000000-0000-4000-9000-000000000000",
8     "serial": 1,
9     "state": "PUBLISHED"
10  },
11  "containers": {
12    "cna": {
13      "providerMetadata": {
14        "orgId": "00000000-0000-4000-9000-000000000000"
15      },
16      "problemTypes": [
17        {
18          "descriptions": [
19            {
20              "lang": "en",
21              "cweId": "CWE-20",
22              "description": "CWE-20 Improper Input Validation",
23              "type": "CWE"
24            }
25          ]
26        }
27      ],
28      "impacts": [
29        {
30          "descriptions": [
31            {
32              "lang": "en",
33              "value": "test"
34            }
35          ]
36        }
37      ]
38    }
39  }
40 }
```

- Add the desired CPE names directly into the CVE record JSON. The cpes array can contain one or more CPE names and exists under the affected array in the same place

that affected products and versions are defined. See the screenshot for an example of a CPE name being used within a CVE record.

```
11  "containers": {
12    "cna": {
13      "providerMetadata": {
14        "orgId": "00000000-0000-4000-9000-000000000000"
15      },
16      "problemTypes": [
17        {
18          "descriptions": [
19            {
20              "lang": "en",
21              "cweId": "CWE-20",
22              "description": "CWE-20 Improper Input Validation",
23              "type": "CWE"
24            }
25          ]
26        }
27      ],
28      "impacts": [
29        {
30          "descriptions": [
31            {
32              "lang": "en",
33              "value": "test"
34            }
35          ]
36        }
37      ],
38      "affected": [
39        {
40          "vendor": "Acme",
41          "product": "ProductY",
42          "cpes": [
43            "cpe:2.3:a:acme:productx:1.0:*:*:*:*:*:*"
44          ],
45          "versions": [
46            {
47              "status": "affected",
48              "version": "1.0"
49            }
50          ],
51          "defaultStatus": "unaffected"
```

9 Additional Information

CVE and NVD

The CVE Program and the NIST National Vulnerability Database (NVD) are separate organizations that share a workflow based on CVE Records. The NVD takes CVE Records as input, performs additional review and analysis, and may make changes or additions. For example, the NVD may add different CVSS or CWE information, add references, and add CPE information. For more information, see [CVEs and the NVD Process](#) and the Collaborative Vulnerability Metadata Acceptance Process ([CVMAP](#)).

CVE Services Credential Security

Anyone with your API key (and your user ID and CNA short name) can access CVE Services with your privileges. Protect your API keys. Consider generating new keys on a periodic basis. If you suspect a key has been compromised, generate a new key and consider disabling affected user accounts. Report any unapproved changes to CVE Records to your Root.

Vulnogram sends your API key in requests and stores the key in your browser, as described in [RISKS](#) (cveClient is another JavaScript CVE Services client).

CVE Services and Record Format Documentation

CVE Services API

<https://cveawg.mitre.org/api-docs/>

CVE Record Format

<https://github.com/CVEProject/cve-schema>

<https://cveproject.github.io/cve-schema/schema/v5.0/docs/>