Vendor Screens

- Overview
- VINCE Pages
  - Dashboard
  - Inbox
    - Message
    - Unread messages
  - Cases
    - Case details
    - View Original Report
    - Vendor Status
    - Vendor status approval
    - Case Discussion
    - Private Message CERT/CC
    - View Draft Vulnerability Note
- My Contact Info
  - Edit Contact Info
- User Management
  - Administrative User Management
  - Adding users
- My Vulnerability Reports
- Report a Vulnerability

Overview

VINCE has a number of capabilities that will guide you through the coordinated vulnerability disclosure process. This document should help you understand how to navigate the various pages that you will see as a vendor using VINCE. The following screens are valid for VINCE 1.0.0.

VINCE Pages

Dashboard

The VINCE Dashboard is the primary location to see active cases associated with your account or vendor.
Inbox

The VINCE Inbox is where you can see messages related to your cases.
Message

Clicking on a message within the VINCE Inbox will allow you to view and reply to the message thread.
Unread messages

When you have one or more unread messages in your Inbox, you will see an indicator along the left side of VINCE.

Cases

VINCE Cases is where you can view cases that are associated with your account or vendor. Each case, which is tracked with a VU# tracking number as CERT has always used, contains one or more related vulnerabilities that may affect your organization.

By default, you will only see active cases. These are the cases that the CERT/CC is actively working on. To view historic cases, you can adjust the Filter by status drop-down menu to control which cases you see.
Case details

Clicking on any particular case will bring you to the case details:
View Original Report

The View Original Report link on the left center section can be used to view the original vulnerability report that was used to create the case.
Vendor Status

For any case that is being handled, the CERT/CC may add your vendor to be associated with the case. For each vulnerability associated with a case, you should indicate whether your organization is Affected or Not Affected and submit the responses accordingly.

For any case, a Vendor Statement can be provided:
Vendor status approval
Once submitted, the CERT/CC will review the vendor status information before it is added to any case.

Case Discussion

For any case that you are involved in, you can view and add to the discussion regarding it. The parties on the right side of the screen will all see the discussion and future parties added to the case will see past discussion. In the example below, the parties involved in the discussion include the CERT/CC (the coordinator), Madison Oliver (the reporter), and XYZ Company (the vendor).
Private Message CERT/CC

If you wish to contact the CERT/CC regarding a case but do not want the other participants in the case to see the message, the Private Message CERT/CC button can be used:

Pressing this button will give you a page where you can send a direct message to the CERT/CC.
View Draft Vulnerability Note
The View the draft vulnerability note link on the right center section can be used to preview what the vulnerability note will look like when it is published.

Software Engineering Institute
CERT Coordination Center

Home > Notes > VU#794047

XYZ-123L is vulnerable to remote command execution

Vulnerability Note VU#794047
Original Release Date:

Overview
XYZ-123L v1.0.0 is vulnerable to remote command execution. The /default.cgi capability in XYZ-123L is exposed to unauthenticated remote users, possibly allowing an attacker to execute remote commands on the vulnerable device.

Description
VU#794047.1 XYZ-123L v1.0.0 is vulnerable to remote command execution. The router contains an exposed CGI that has a ping function that incorrectly handles newline characters and will execute any arguments after the newline on the device with root privileges.

My Contact Info

VINCE My Contact Info is where you can edit details about your contact information.
Edit Contact Info

My Contact Info

XYZ Company

Email Lists

PGP Keys

Location

Phone Numbers

Website

vince Users

madisonqoliver@gmail.com (MQO XYZ Analyst)
Press **Edit My Contact Info** to enter or modify contact information for your account.

Here a user can edit the following pieces of information for their account:

- Organization logo
- Email lists
- PGP keys
- Location
- Phone numbers
- Website

For each attribute above, the **Public?** switch can be used to toggle whether this information is viewable by the public. Currently, this means that the information is viewable to other VINCE users, but in the future this information may be made public.

**User Management**

VINCE **User Management** can be used to manage the members of a vendor's contact list. If your account has not been determined to be the group administrator for the vendor you are associated with, you will not be able to perform any actions here. If you are the individual who should have administrative access over the vendor's user management, click the **contact CERT/CC** link to send a message to request this access.
**Administrative User Management**

If your administrator access level has been approved, you will see a screen similar to this:

- You must be the designated group administrator to view information about users in your group. Please contact CERT/CC to request group administrator privileges.
Adding users

By clicking the Invite User button, a group administrator can invite new users to use VINCE as part of the vendor that is being managed, which is XYZ Company in this case.
My Vulnerability Reports

For most vendors using VINCE, the **My Vulnerability Reports** part of VINCE will not be used. This part of VINCE is used for vulnerabilities reported using your VINCE account. In other words, if you haven't reported a vulnerability using VINCE, then you should expect this part of VINCE to look like this:
Report a Vulnerability

If you have a vulnerability to report to the CERT/CC, you can use the Report a Vulnerability link.
Vulnerability Reporting Form

You are logged in as Vendor.

Vulnerability Information

Have you attempted to contact the vendor? *
- Yes
- No

Vendor Name

Do you believe multiple vendors are affected? *
- Yes
- No

What is the name of the affected product or software? *
This field will be used in the subject and/or body of an acknowledgment email from CERT/CC to help identify this report with its tracking number. Please DO NOT include any sensitive information in this field. Give the full product