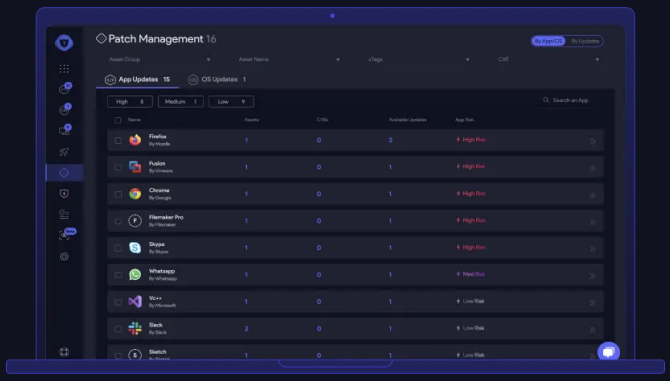
vicarius.io

0-Day Detection

vRx's 0-Day analysis uses a proactive approach that continuously analyzes, predicts and identifies novel binary level threats. Don't wait for your software to get hacked. Protect your organization with vRx.



Threat Prediction

vRx's 0-day analysis engine automatically characterizes exploited areas in any binary software. Leveraging this knowledge, vRx identifies similar vulnerabilities in your applications, analyzes them, and informs you about potential weaknesses before hackers find them.

0-Day Use Cases

Beyond CVEs

Relying entirely on public CVE disclosures leaves your organization vulnerable. By comparing binary pieces to existing threat categories, vRx identifies potential software vulnerabilities that can put your applications at risk of being exploited. vRx enables you to cover the security gaps.

Proprietary Software

Many companies use proprietary, legacy, or unsupported software--all of which can be exploited and may lead to complete organizational failure. vRx identifies threats in any software within your organization's digital environment, reducing overall risk.

Get in Front of the Patch Cycle

The CVE disclosures cycle is a waiting game. The time spent waiting on the subsequent patches can leave your organization open to cyber attacks for months at a time. vRx allows you to break free from the patch cycle and increase your organization's efficiency, reducing your overall security risk level.

How It Works

vRx collects and analyzes software binaries for patterns to determine vulnerable spots in the libraries. Like DNA mapping, it identifies weak genes, i.e., a predicted vulnerability, based on the environment it analyzes. vRx's detection engine is composed of 3 parts:

01

Detect targets

Examines the behavior of malware samples to see which parts of the software they are abusing.

02

Find similarity

A machine-learning algorithm finds similarities between them to identify a common target characterization.

03

Create patterns

Common target characterization patterns are used to hunt for similar targets on every application in the organization.