FORTINET
Training Institute

FORTINET
CERTIFIED
SOLUTION
SPECIALIST
Security
Operations

Security Operations Analyst

Attack Surface and Vectors

FortiAnalyzer 7.4

Last Modified: 22 January 2025

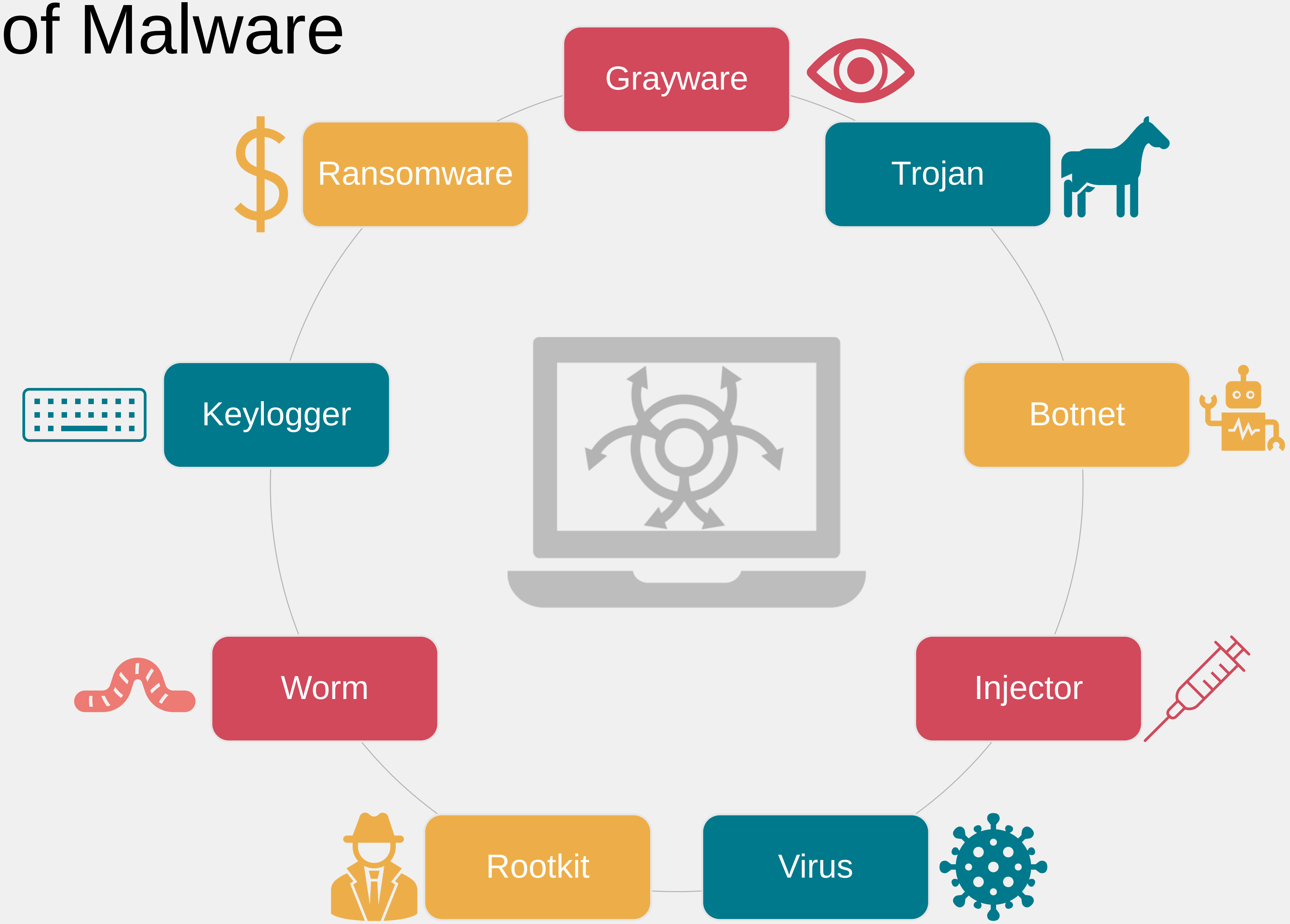
Social Engineering

- Refers to a range of attacks that manipulate users, including:
  - Baiting
  - Scareware
  - Phishing
  - Pretexting
  - Tailgating

- The victims are fooled into performing dangerous actions

- Information gathered from reconnaissance can make the attacker seem more trustworthy

Types of Malware



Grayware

Trojan

Botnet

Injector

Virus

Rootkit

Worm

Keylogger

Ransomware

FORTINET

Training Institute

Compromised Credentials

Data Breach

Keylogging

Phishing

Password Manager

Note: You can visit websites such as https://monitor.mozilla.org or https://haveibeenpwned.com to see if your email account has been part of a data breach.

Credential Attacks

Attack Name	Description
Brute force	- Try all combinations for a match
Password spraying	- Target multiple hosts with limited attempts (to avoid detection)
Dictionary	- Use a list of compiled passwords to find a match
Credential stuffing	- Use information from data breaches to find a match
Man-in-the-middle	- Intercept traffic to steal sensitive information
Rainbow table	- Precompile a list of passwords into hashes to find a matching hash

Credentials Best Practices

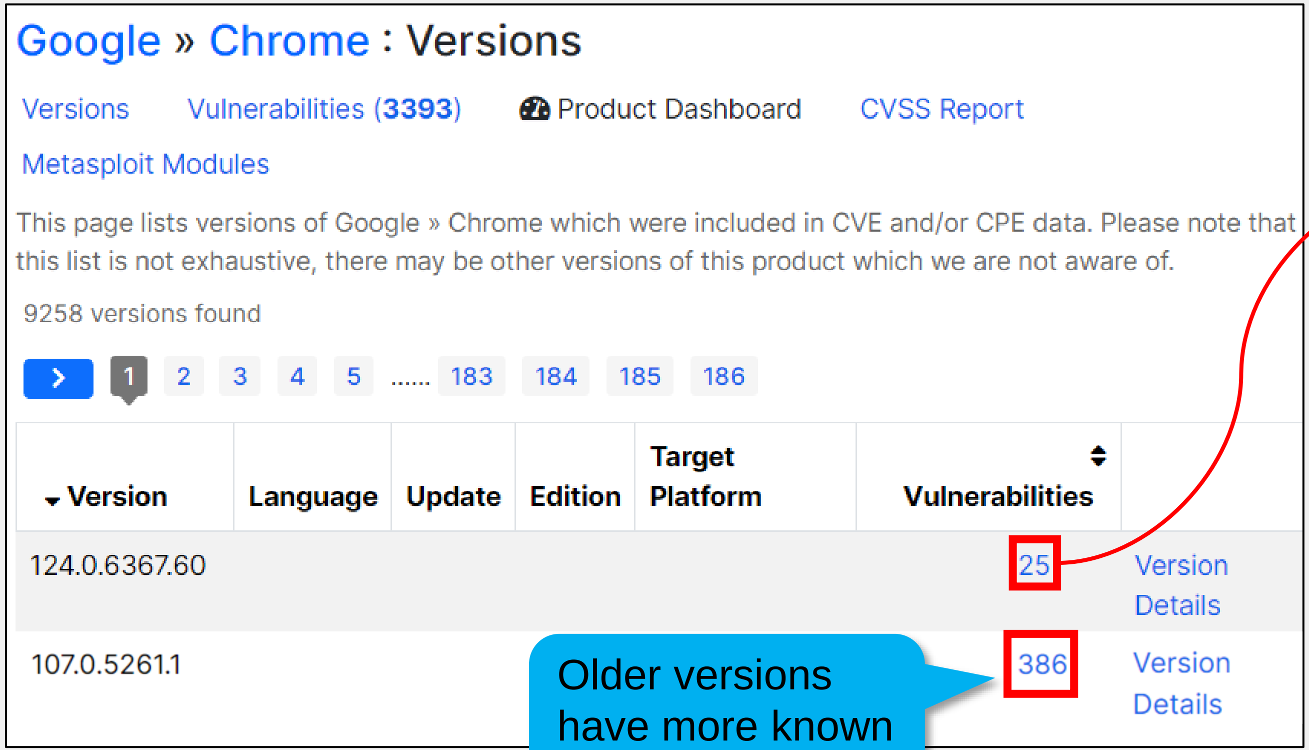
- As an organization:
  - Ban recycling passwords
  - Enforce password complexity
  - Enforce MFA across the organization
  - Set a short password validity period
  - Set a low limit for failed login attempts

- As an end user:
  - Don’t use the same passwords for personal and business accounts
  - Check to see if the password has been compromised (using online search engines)
  - Check to see if your email account has been involved in data breaches
  - Never write down any passwords
  - Do not share MFA codes
  - Do not share your cell phone

Software Vulnerabilities

- Search for software versions of assets in your organization and view a list of vulnerabilities

- Not all vulnerabilities are critical, but you need to be aware of all risks



Google » Chrome : Versions

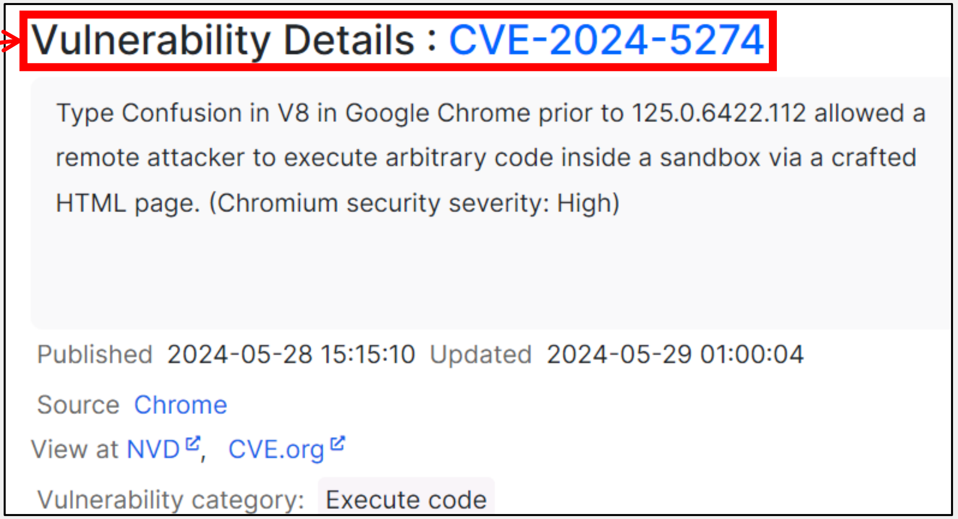
Versions Vulnerabilities (**3393**) Product Dashboard CVSS Report Metasploit Modules

This page lists versions of Google » Chrome which were included in CVE and/or CPE data. Please note that this list is not exhaustive, there may be other versions of this product which we are not aware of.

9258 versions found

Version	Language	Update	Edition	Target Platform	Vulnerabilities	
124.0.6367.60					25	Version Details
107.0.5261.1					386	Version Details

Older versions have more known vulnerabilities



Vulnerability Details : CVE-2024-5274

Type Confusion in V8 in Google Chrome prior to 125.0.6422.112 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: High)

Published 2024-05-28 15:15:10 Updated 2024-05-29 01:00:04

Source Chrome

View at NVD, CVE.org

Vulnerability category: Execute code

FORTINET
Training Institute

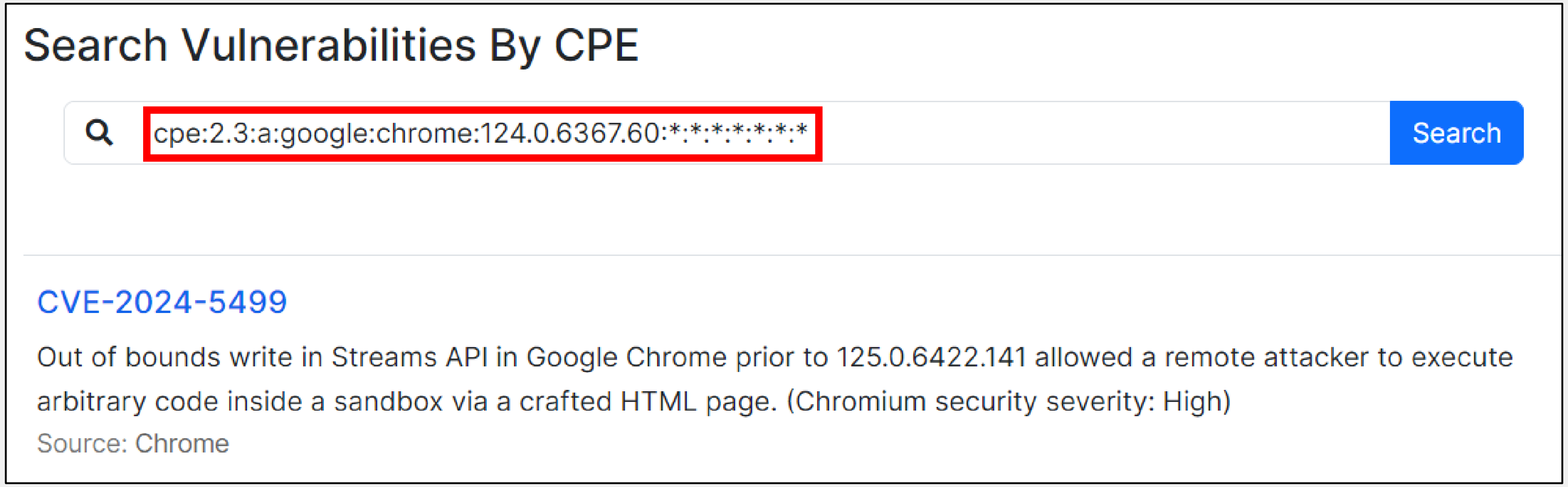
Software Vulnerabilities (Contd)

- Common Platform Enumeration (CPE) is a standardized scheme to identify assets

- The CPE 2.3 format follows this syntax:

```
cpe:<cpe_version>:<part>:<vendor>:<product>:<version>:<update>:<edition>:<language>:<sw_edition>
:<target_sw>:<target_hw>:<other>
```

- You can also search vulnerabilities based on a CPE string:



Search Vulnerabilities By CPE

cpe:2.3:a:google:chrome:124.0.6367.60:*:*:*:*:*:*:*

CVE-2024-5499

Out of bounds write in Streams API in Google Chrome prior to 125.0.6422.141 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: High)

Source: Chrome

Review

- ✓Describe the attack surface
- ✓Describe how to identify the attack surface
- ✓Describe how to reduce the attack surface
- ✓Describe common attack vectors
- ✓Describe security best practices against attack vectors
- ✓Describe defenses against attack vectors
- ✓Describe how to capture traffic on Fortinet devices
- ✓Describe how to capture traffic on an endpoint
- ✓Describe how to use Wireshark to analyze packet captures