Common vulnerabilities and exposures

We've discussed before that security is a team effort.
Did you know the group extends well beyond a single security team?
Protecting information is a global effort!

When it comes to vulnerabilities, there are actually online public libraries.
Individuals and organizations use them to share and document common vulnerabilities and exposures.
We've been focusing a lot on vulnerabilities.
Exposures are similar, but they have a key difference.
While a vulnerability is a weakness of a system, an exposure is a mistake that can be exploited by a threat.

For example, imagine you're asked to protect an important document.
Documents are vulnerable to being misplaced.
If you laid the document down near an open window, it could be exposed to being blown away.

One of the most popular libraries of vulnerabilities and exposures is the CVE list.
The common vulnerabilities and exposures list, or CVE list, is an openly accessible dictionary of known vulnerabilities and exposures.
It is a popular resource.

Many organizations use a CVE list to find ways to improve their defenses.
The CVE list was originally created by MITRE corporation in 1999.
MITRE is a collection of non-profit research and development centers.
They're sponsored by the US government.
Their focus is on improving security technologies around the world.

The main purpose of the CVE list is to offer a standard way of identifying and categorizing known vulnerabilities and exposures.
Most CVEs in the list are reported by independent researchers, technology vendors, and ethical hackers, but anyone can report one.
Before a CVE can make it onto the CVE list, it first goes through a strict review process by a CVE Numbering Authority, or CNA.

A CNA is an organization that volunteers to analyze and distribute information on eligible CVEs.
All of these groups have an established record of researching vulnerabilities and demonstrating security advisory capabilities.
When a vulnerability or exposure is reported to them, a rigorous testing process takes place.

The CVE list tests four criteria that a vulnerability must have before it's assigned an ID.
First, it must be independent of other issues.
In other words, the vulnerability should be able to be fixed without having to fix something else.
Second, it must be recognized as a potential security risk by whoever reports it.
Third, the vulnerability must be submitted with supporting evidence.
And finally, the reported vulnerability can only affect one codebase, or in other words, only one program's source code.
For instance, the desktop version of Chrome may be vulnerable, but the Android application may not be.
If the reported flaw passes all of these tests, it is assigned a CVE ID.

Vulnerabilities added to the CVE list are often reviewed by other online vulnerability databases.
These organizations put them through additional tests to reveal how significant the flaws are and to determine what kind of threat they pose.
One of the most popular is the NIST National Vulnerabilities Database.

The NIST National Vulnerabilities Database uses what's known as the common vulnerability scoring system, or CVSS, which is
a measurement system that scores the severity of a vulnerability.
Security teams use CVSS as a way of calculating the impact a vulnerability could have on a system.
They also use them to determine how quickly a vulnerability should be patched.

The NIST National Vulnerabilities Database provides a base score of CVEs on a scale of 0-10.
Base scores reflect the moment a vulnerability is evaluated, so they don't change over time.
In general, a CVSS that scores below a 4.0 is considered to be low risk and doesn't require immediate attention.
However, anything above a 9.0 is considered to be a critical risk to company assets that should be addressed right away.

Security teams commonly use the CVE list and CVSS scores as part of their vulnerability management strategy.
These references provide recommendations for prioritizing security fixes, like installing software updates before patches.

Libraries like the CVE list, help organizations answer questions. Is a vulnerability dangerous to our business?
If so, how soon should we address it?
These online libraries bring together diverse perspectives from across the world.
Contributing to this effort is one of my favorite parts of working in this field.
Keep gaining experience, and I hope you'll participate too!

Revision #1
Created 2023-08-07 13:22:02 UTC by naruzkurai
Updated 2023-08-15 18:44:13 UTC by naruzkurai