**The Patch Factory**

Global Infrastructure for Managing Cybersecurity Vulnerabilities

**Initial Disclosure**

- **Bad Guys**: Malicious actors using the vulnerability “in the wild”
- **3rd Party Bug Hunters/Researchers**: Private security consultants, testers, and researchers
- **DHS Research**: Security testing and research performed or sponsored by DHS
- **In-House Research & Testing**: Security testers and researchers who test their own products & systems

**Analyses & Coordination**

- **CVE ID Assignment**: Each vulnerability is assigned a unique ID number per the CVE Counting Rules
- **Coordination**: Reaching out to contact networks and trusted communities
- **Triage & Validation**: Is this a real vulnerability? Are the discoverer’s claims accurate?

**Assessing Severity**

A Common Vulnerability Severity Score (CVSS) is calculated for each vulnerability. Other factors may also come into play, such as how widespread the vulnerability is and what types of impacts might be caused if the vulnerability is exploited (or if exploitation is already occurring).

**Disclosure & Publishing**

The vulnerability is made public, usually at the same time as a software update to fix the issue. The MITRE CVE and NIST NVD entries are created and updated as more references and data become available.

**Post-Disclosure Coordination**

After publication, other potentially affected vendors may come forward to provide or request additional info, expanding the contact network.

**Remediation Phase**

- **Patches/Updates** and published Advisories
  - **Simple Fixes**: e.g., local bugs in websites or web services
  - **Scanning Signatures** to find vulnerable systems
  - **Intrusion Signatures** to detect exploit attempts
  - **Countermeasures** or other mitigations (Not everything can or will be patched, so other countermeasures are necessary to prevent exploitation)

**These processes are relied upon by software makers, cybersecurity teams, and system administrators all over the world.**

---

cisa.gov