THE PATCH FACTORY

Global Infrastructure for Managing Cybersecurity Vulnerabilities

VULNERABILITY DISCOVERY

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

INITIAL DISCLOSURE

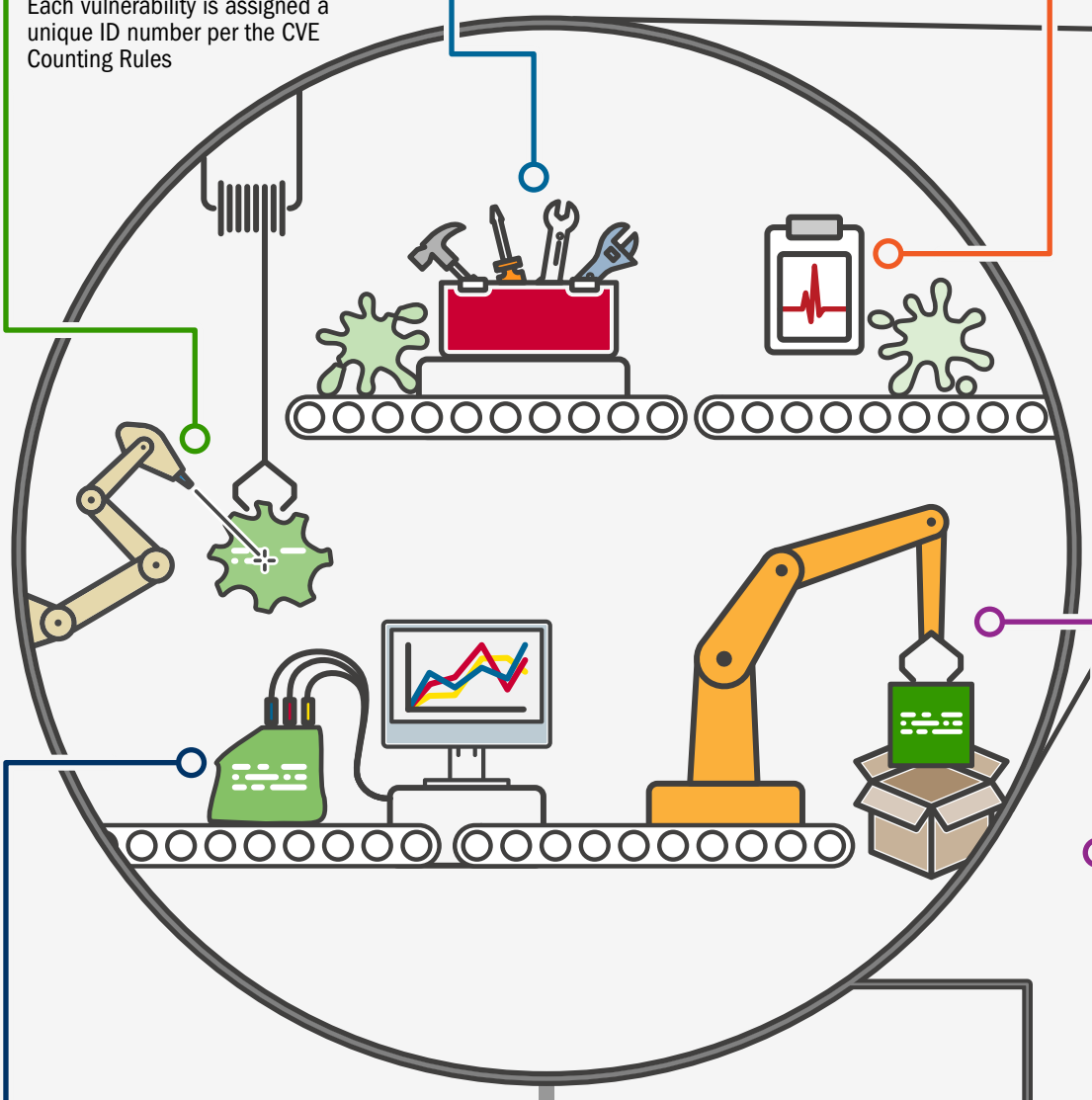
- BUG BOUNTY PROGRAMS
- CISA/CSD
- COMPUTER SECURITY INCIDENT RESPONSE TEAMS (CSIRTs)
- CVE NUMBERING AUTHORITIES
- MITRE CVE
- CONFERENCE BRIEFINGS/ PRESENTATIONS
- MAILING LISTS/ SOCIAL MEDIA
- PRODUCT SECURITY INCIDENT RESPONSE TEAMS (PSIRTs)
- SOFTWARE ENGINEERING INSTITUTE

ANALYSIS AND COORDINATION

COORDINATION
Reaching out to contact networks and trusted communities

TRIAGE & VALIDATION
Is this a real vulnerability? Are the discoverer's claims accurate?

CVE ID ASSIGNMENT
Each vulnerability is assigned a unique ID number per the CVE Counting Rules



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.

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).

POST-DISCLOSURE COORDINATION
After publication, other potentially affected vendors may come forward to provide of 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 sometimes necessary to prevent exploitation)

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