Cassandra

A system to provide customized notifications of vulnerabilities

by Pascal Meunier

Thanks to

- Peter Mell (NIST)
- Vince Koser and Kent Wert (CERIAS)
- All of the contributors to the CVE effort

Profile

- Of a host or network, or personal interest
- List of applications and operating systems
- Unlimited number of applications

Searches

- Interval
  - All, 1 year, 6, 3, or 1 month
- Incremental (new results only)

Email

- Either a simple notice
- Or a list of vulnerabilities
    - Same as incremental search (emailed)

Comment System

- Per vulnerability
- Quality Assurance by votes
- One vote/user/comment

Data source

- ICAT by NIST (icat.nist.gov)
    - Based on the CVE
- CVE based on public sources

Status

- 430 Users
- 446 profiles
  - 210 requesting email notification

Totals since 12/27/00

- 3217 emails sent
- 11605 records served
- 718 new CVE entries

Future Improvements

- More frequent updates from ICAT!
- More frequent updates from CVE
- Patch Notifications

Vendors of products with most hits

- Records served/vendor in last 2 months
- Theory: Vulnerabilities/vendor X usage

  = Vendor responsibility
- New measurement of "secure"

Rankings

- Microsoft: 3.6x more than #2 (04/25/01)
- Improving: was 10x (11/00)
- Or others getting worse?

Operating Systems

- Operating System vendors dominate top 10
- All Unix vendors: 4988 vs 3346 Microsoft (incl. applications)
- Why aren't OSes more secure than apps?