

Software Errors – SANS Top 25

Mahesh Saptarshi

Agenda

- Software errors – security implications
- Other efforts at classifying
- SANS Top 25
- Q&A

Software Errors – security implications

Software Errors – security implications

- Arbitrary malicious code execution
- Unauthorized file access
- Privacy breach
- Access to data/service blocked
- Sensitive data leakage
- Monetary losses

Software Errors

- Accessing beyond the available memory
- Indexing memory array beyond its size
- Not checking error returns from APIs
- Memory leaks – allocate but not free
- Which file to read/write, by whom? What is the path?
- Indicated data size does not match actual data
- In-band commands to interpreters
- Undetected Data corruption
- Fake data source
- Data leakage through log files, config files, error messages, etc

Other classification schemes

- OWASP Top 10 web application security issues
- 19 deadly sins of software security – Howard, LeBlanc, Viega
- Software vulnerability guide
- Building secure software
- MS-SDL

SANS Top 25

<http://www.sans.org/top25errors/>

Why is this important?

- Software Industry agreement based on empirical data
- Large participation
- SANS sponsorship
- How will this list be used?
- What are other resources?

<http://www.sans.org/top25errors/#s5>

SANS Top 25 – How will this be used?

“

...

- * Software buyers will be able to buy much safer software.
- * Programmers will have tools that consistently measure the security of the software they are writing.

”

...

SANS Top 25

SANS Top 25 divided in 3 broad categories

A) **Insecure Interaction Between Components**

B) **Risky Resource Management**

C) **Porous Defenses**

1. Improper Input Validation
2. Improper Encoding or Escaping of Output
3. Failure to Preserve SQL Query Structure (aka 'SQL Injection')
4. Failure to Preserve Web Page Structure (aka 'Cross-site Scripting')
5. Failure to Preserve OS Command Injection
6. Cleartext Transmission of Sensitive Information
7. Cross-Site Request Forgery (CSRF)
8. Race Condition
9. Error Message Information disclosure

10. Failure to Constrain Operations within the Bounds of a Memory Buffer
11. External Control of Critical State Data
12. External Control of File Name or Path
13. Untrusted Search Path
14. Failure to Control Generation of Code (aka 'Code Injection')
15. Download of Code Without Integrity Check
16. Improper Resource Shutdown or Release
17. Improper Initialization
18. Incorrect Calculation

19. Improper Access Control (Authorization)
20. Use of a Broken or Risky Cryptographic Algorithm
21. Hard-Coded Password
22. Insecure Permission Assignment for Critical Resource
23. Use of Insufficiently Random Values
24. Execution with Unnecessary Privileges
25. Client-Side Enforcement of Server-Side Security

My Top 10

1. Failure to Constrain Operations within the Bounds of a Memory Buffer
2. Insecure Permission Assignment for Critical Resource
3. Execution with Unnecessary Privileges
4. Cleartext Transmission of Sensitive Information
5. Use of a Broken or Risky Cryptographic Algorithm
6. External Control of File Name or Path

Top 10

7. Download of Code Without Integrity Check

8. Improper Input Validation

- Failure to Preserve SQL Query Structure (aka 'SQL Injection')
- Failure to Preserve Web Page Structure (aka 'Cross-site Scripting')
- Failure to Preserve OS Command Injection

9. Hard-Coded Password

10. Use of Insufficiently Random Values

Skill and Tools

Skills

- Application pen-test expertize
- Multiple platforms expertize
 - Windows, Linux, AIX, Solaris, HP-UX
- Network fuzzers
- Strong programming and scripting skills
- Training material for secure coding, configuration and security QA

Tools

- MetaSploit
- Google RAT proxy
- Scarab
- WebGoat
- Nessus
- Nmap
- Firewalk

Thank You!

Mahesh Saptarshi
amahesh@gmail.com