Security of Networks, Services, and Systems

Quick Intro to Vulnerabilities

Ricardo Morla

FEUP – SSR/M.EEC, SR/M.EIC

Definition

- Weaknesses that allow an attacker to gain access to information, control over a system, or deny service access to others
  - Set of vulnerabilities is known as attack surface
- Successful exploitation requires:
  - Susceptibility or flaw of a system (vulnerability)
  - Attacker access to the vulnerability
  - Attacker capability to exploit the vulnerability

Types of vulnerabilities

- **Flaws in algorithms and protocols**
    - When the cipher is known to be vulnerable to cryptanalysis
    - When the block operation or network protocol is not secure (e.g. key exchange)
- Implementation bugs
- Accessible attack points
- User-related
- Denial of service

Types of vulnerabilities

- Flaws in algorithms and protocols
- **Implementation bugs**
  - Incorrect implementation of crypto algorithm that reduces brute force attack space
  - Memory safety violations - buffer overflow, dangling pointers
  - Input validation - SQL injection, cross-side scripting
  - Race conditions - time of check to time of use
  - Privilege confusion - cross-site request forgery
  - Privilege escalation - horizontal, vertical & jailbreak
- Accessible attack points
- User-related
- Denial of service

Types of vulnerabilities

- Flaws in algorithms and protocols
- Implementation bugs
- **Accessible attack points**
  - TCP ports opened by default system services not firewalled
  - Sharing services with no authentication and access control
  - Operating system access control limitations (e.g. no root password)
- User-related
- Denial of service

Types of vulnerabilities

- Flaws in algorithms and protocols
- Implementation bugs
- Accessible attack points
- **User-related**
  - Poorly chosen or not securely stored passwords
  - Email viruses, phishing, social network
- Denial of service

Types of vulnerabilities

- Flaws in algorithms and protocols
- Implementation bugs
- Accessible attack points
- User-related
- **Denial of service**
  - This vulnerability is always present
  - As long as the service can be accessed by potential attackers
  - Can also see it as threat

References to databases of types, instances, and exploits of vulnerabilities

- **CWE** - Common Weakness Enumeration (type of vulnerability)

  https://cwe.mitre.org/

- **CVE** - Common Vulnerabilities and Exposures (instance of vulnerability, exploit)

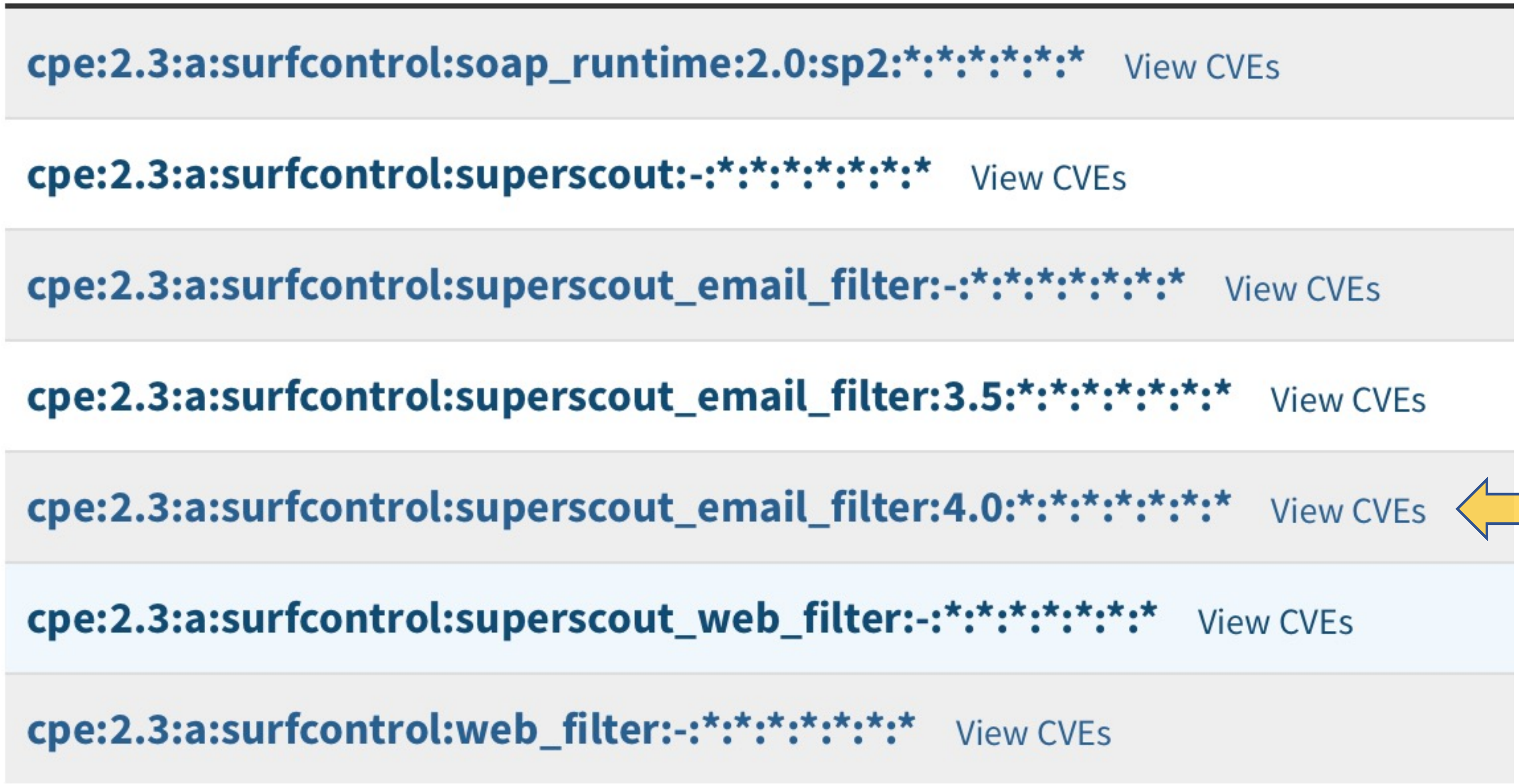
  https://cve.mitre.org

- **CPE** – Common Platform Enumeration (id platform subject to vulnerability)

  https://nvd.nist.gov/products/cpe

CPE example

https://nvd.nist.gov/products/cpe/search/results?namingFormat=2.3&keyword=SurfControl



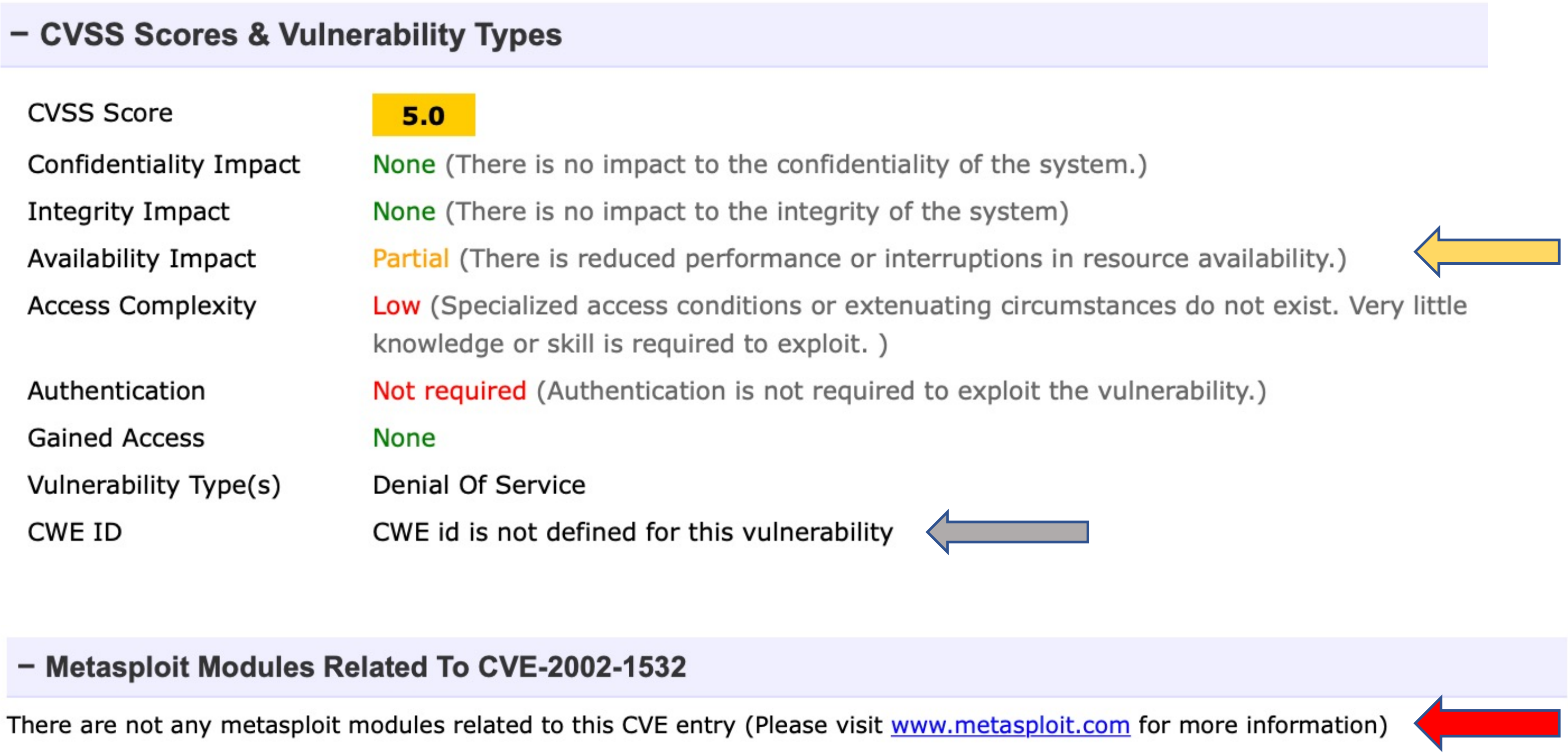
cpe:2.3:a:surfcontrol:soap_runtime:2.0:sp2:*:*:*:*:*:*	View CVEs
cpe:2.3:a:surfcontrol:superscout:-:*:*:*:*:*:*:*	View CVEs
cpe:2.3:a:surfcontrol:superscout_email_filter:-:*:*:*:*:*:*:*	View CVEs
cpe:2.3:a:surfcontrol:superscout_email_filter:3.5:*:*:*:*:*:*:*	View CVEs
cpe:2.3:a:surfcontrol:superscout_email_filter:4.0:*:*:*:*:*:*:*	View CVEs
cpe:2.3:a:surfcontrol:superscout_web_filter:-:*:*:*:*:*:*:*	View CVEs
cpe:2.3:a:surfcontrol:web_filter:-:*:*:*:*:*:*:*	View CVEs

CVE-2002-1532

CVE example

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2002-1532

The administrative web interface (STEMWADM) for SurfControl SuperScout Email Filter allows **remote attackers** to cause a **denial of service** (resource exhaustion) via a GET request without the terminating /r/n/r/n (CRLF) sequence, which causes the interface to **wait for the sequence and blocks other users** from accessing it.



− CVSS Scores & Vulnerability Types

CVSS Score	**5.0**
Confidentiality Impact	None (There is no impact to the confidentiality of the system.)
Integrity Impact	None (There is no impact to the integrity of the system)
Availability Impact	Partial (There is reduced performance or interruptions in resource availability.)
Access Complexity	Low (Specialized access conditions or extenuating circumstances do not exist. Very little knowledge or skill is required to exploit.)
Authentication	Not required (Authentication is not required to exploit the vulnerability.)
Gained Access	None
Vulnerability Type(s)	Denial Of Service
CWE ID	CWE id is not defined for this vulnerability

− Metasploit Modules Related To CVE-2002-1532

There are not any metasploit modules related to this CVE entry (Please visit www.metasploit.com for more information)

CWE example

https://cwe.mitre.org/data/definitions/166.html

- CWE-166: Improper Handling of Missing Special Element
- Special case of:
  - Improper Check or Handling of Exceptional Conditions - (CWE703)
- Relevant to the weakness view:
  - Research Concepts
  - Software Development (Data processing Errors)
- Observed example:
  - CVE-2002-1532
  - HTTP GET without `\r\n\r\n CRLF` sequences causes product to wait indefinitely and prevents other users from accessing it

Security of
Networks, Services, and Systems

Quick Intro to Vulnerabilities

Ricardo Morla

FEUP – SSR/M.EEC, SR/M.EIC