VULNERABILITY DB

Description

БАЗОВАЯ МЕТРИКА

- базовая метрика уязвимостей

- cvss BaseScore = round_to_1_decimal(((0.6*Impact)+(0.4*Exploitability)-1.5)*f(Impact))

VULNERABILITY DATABASE

- Банк данных угроз безопасности информации ФСТЭК (http://bdu.fstec.ru/vul) (BISA)
- CVE MITRE
- NVD
- OSVBD
- VNB
- BID
- ISS X-FORCE
- …
- + коммерческие БД

CVE

- CVE 2014-xxxx
- CVE 2015-xxxxx
- CVE - общепринятый стандарт именования уязвимостей, присутствующих в коммерческих и open-source программных продуктах.

ВЕКТОР УЯЗВИМОСТИ

- Вектор: AV:N/AC:L/Au:N/C:N/I:N/A:C

- Access Vector: Network — возможность доступа к объекту исключительно через сеть.
- Access Complexity: Low — сложность доступа к ресурсу: низкая.
- Authentication: None – для эксплуатации не нужна авторизация.
- Confidentiality Impact: None — влияние на разглашение критичной информации.
- Integrity Impact: None — нарушение целостности. Понятие “целостность" связано с достоверностью и точностью информации.
- Availability Impact: Complete — атаки, потребляющие пропускную способность сети, циклы процессора или дисковое пространство, которые влияют на доступность системы.

ВРЕМЕННЫЕ МЕТРИКИ

- Изменяются во времени
- Exploitability (E) — возможность эксплуатации.
- Remediation Level (RL) — уровень исправления.
- Report Confidence (RC) — степень достоверности отчета.

СОВМЕСТИМОСТЬ

- Unix Known Problem List, Internal Sun Microsystems Bug List, каталоги служб реагирования на компьютерные инциденты CERT ранних версий.
- Список совместимости систем классификаций:
- CVE: ISS, BID, Secunia, SecurityTracker, OSVDB
- BID: CVE, Bugtraq, ISS, Secunia, SecurityTracker, OSVDB
- ISS: CVE, BID, Secunia, SecurityTracker, OSVDB
- Secunia: CVE, OSVDB
- SecurityTracker: CVE, OSVDB, Nessus
- Nessus: CVE, BID, OSVDB
- OSVDB: CVE, BID, Secunia, SecurityTracker, ISS, Nessus, Snort