Branden Solomon
9/26/24
FCNS

FCNS Class Assignment

NIST Vulnerability Database

1. DNS Poisoning

CVE Number: CVE-2020-25685

Publish date: 01/20/2021

CVSS 3.x Severity

Base Score: 3.7 Low

Exploitability Metrics:

- **Attack Vector (AV)**: N (Network)
- **Attack Complexity (AC)**: H (High)
- **Privileges Required (PR)**: N (None)
- **User Interaction (UI)**: N (None)
- **Scope (S)**: U (Unchanged)

Impact Metrics:

- **Confidentiality Impact (C)**: N (None)
- **Integrity Impact (I)**: L (Low)
- **Availability Impact (A)**: N (None)

Attack Levels:

- **Low Severity**: Redirects users to a benign site, causing minor issues.
- **Medium Severity**: Users are directed to phishing sites, risking credential theft.
- **High Severity**: Users are misled to a financial site, resulting in significant losses.
- **Critical Severity**: Affects multiple domains, leading to widespread data breaches.

OSI Model Responsibility:

- **Layer 3 (Network Layer)**: The attack exploits how devices resolve domain names.
- **Layer 7 (Application Layer)**: Affects application-level functions by misleading users and applications.

3 Entities of the Computer Device

User Devices: Users may fall victim to phishing, disrupting their activities.

Servers: Compromised DNS servers can mislead all clients, affecting reliability.

Network Infrastructure: Impacts overall network operations, causing connectivity issues.

2. DNS Hijacking

CVE Number: CVE-2022-47758

Publish date: 04/26/2023

CVSS 3.x Severity

Base Score: 9.8 Critical

Exploitability Metrics

- **Attack Vector**: Network (N)
- **Attack Complexity**: Low (L)
- **Privileges Required**: None (N)
- **User Interaction**: None (N)
- **Scope**: Unchanged (U)

Impact Metrics

- **Confidentiality**: High (H)
  Sensitive data can be exposed.
- **Integrity**: High (H)
  Data can be altered by attackers.
- **Availability**: High (H)
  Significant disruptions to services.

Attack Levels

- **Low**: Redirects to harmless sites, causing minor issues.
- **Medium**: Users are sent to phishing sites, risking credential theft.
- **High**: Redirects to fraudulent financial sites, leading to financial loss.
- **Critical**: Affects multiple domains, resulting in widespread data breaches.

3 Entities of the Computer Device

- **User Devices**: Credential theft and security risks.
- **Servers**: Compromised DNS impacts reliability.
- **Network Infrastructure**: Disrupts connectivity and normal operations.

OSI Model Responsibility

- **Layer 3 (Network Layer)**: Exploits DNS resolution processes.
- **Layer 7 (Application Layer)**: Misleads applications and users.

3. Man in the Middle

CVE Number: CVE-2024-37068

Publish date: 09/07/2024

CVSS 3.x Severity

Base Score: 7.5 high

Exploitability Metrics

- **Attack Vector (AV)**: N (Network)
- **Attack Complexity (AC)**: L (Low)
- **Privileges Required (PR)**: N (None)
- **User Interaction (UI)**: N (None)
- **Scope (S)**: U (Unchanged)

Impact Metrics

- **Confidentiality Impact (C)**: H (High)
- **Integrity Impact (I)**: H (High)
- **Availability Impact (A)**: H (High)

Attack Levels

- **Low**: Minor data interception with little impact.
- **Medium**: Unauthorized access to user credentials.
- **High**: Significant exposure to sensitive data.
- **Critical**: Widespread breaches affecting multiple systems.

3 Entities of the Computer Device

- **User Devices**: Risk of credential theft.
- **Servers**: Potential data exposure.
- **Network Infrastructure**: Disrupts normal operations.

OSI Model Responsibility

- **Layer 1 (Physical Layer)**: Attackers may tap into physical connections, intercepting data directly through compromised cables or network devices.
- **Layer 5 (Session Layer)**: Vulnerabilities can disrupt session establishment and management, allowing attackers to hijack or manipulate active sessions.

4. Session Replay

CVE Number: CVE-2024-3297

Publish date: 07/24/2024

CVSS 3.x Severity

Base Score: 6.5 medium

Exploitability Metrics

- **Attack Vector (AV)**: N (Network)
- **Attack Complexity (AC)**: L (Low)
- **Privileges Required (PR)**: N (None)
- **User Interaction (UI)**: N (None)
- **Scope (S)**: U (Unchanged)

Impact Metrics

- **Confidentiality Impact (C)**: M (Medium)
- **Integrity Impact (I)**: L (Low)
- **Availability Impact (A)**: N (None)

Attack Levels

- **Low**: Interception of non-sensitive session data.
- **Medium**: Replay of user sessions leading to unauthorized actions.
- **High**: Significant unauthorized access to user accounts.
- **Critical**: Compromise of sensitive data across multiple accounts.

3 Entities of the Computer Device

- **User Devices**: Risk of unauthorized actions and data exposure.
- **Servers**: Potential misuse of user sessions, affecting trust.
- **Network Infrastructure**: This may disrupt normal session management.

OSI Model Responsibility

- **Layer 3 (Network Layer)**: Exploits network traffic to capture sessions.
- **Layer 7 (Application Layer)**: Affects session management and application integrity.

5. Man in the Browser

CVE Number: CVE-2024-28100

Publish date: 09/02/2024

CVSS 3.x Severity

Base Score: 5.4 medium

Exploitability Metrics

- **Attack Vector (AV)**: N (Network)
- **Attack Complexity (AC)**: L (Low)

- **Privileges Required (PR)**: N (None)
- **User Interaction (UI)**: N (None)
- **Scope (S)**: U (Unchanged)

Impact Metrics

- **Confidentiality Impact (C)**: M (Medium)
- **Integrity Impact (I)**: H (High)
- **Availability Impact (A)**: N (None)

Attack Levels

- **Low**: Minor alterations to browser behavior with little impact.
- **Medium**: Interception of user input, leading to unauthorized actions.
- **High**: Significant manipulation of transactions or data.
- **Critical**: Widespread data theft and financial fraud across multiple accounts.

3 Entities of the Computer Device

- **User Devices**: Risk of data manipulation and unauthorized actions.
- **Servers**: Compromised transactions can undermine trust in services.
- **Network Infrastructure**: This will may interfere with secure communications.

OSI Model Responsibility

- **Layer 3 (Network Layer)**: Exploits network communications to inject malicious scripts.
- **Layer 7 (Application Layer)**: Directly affects the browser's handling of user input and transactions.

6. DDOS

CVE Number: CVE-2023-22397

Publish date: 01/12/2023

CVSS 3.x Severity

Base Score: 6.1 medium

Exploitability Metrics

- **Attack Vector (AV)**: N (Network)
- **Attack Complexity (AC)**: L (Low)
- **Privileges Required (PR)**: N (None)
- **User Interaction (UI)**: N (None)
- **Scope (S)**: U (Unchanged)

Impact Metrics

- **Confidentiality Impact (C)**: M (Medium)
- **Integrity Impact (I)**: L (Low)
- **Availability Impact (A)**: N (None)

Attack Levels

- **Low**: Minor data exposure with negligible impact.
- **Medium**: Unauthorized access to moderate information, posing some risk.
- **High**: Significant data access that could lead to more serious breaches.
- **Critical**: Widespread impact affecting sensitive data across multiple systems.

Impact on Computing Devices

- **User Devices**: Potential risk of unauthorized information access.
- **Servers**: Possible data integrity issues affecting trustworthiness.
- **Network Infrastructure**: May result in minor disruptions in normal operations.

OSI Model Responsibility

- **Layer 2 (Data Link Layer):** Potential for flooding the link layer with excessive traffic, affecting MAC address processing and local network performance.
- **Layer 4 (Transport Layer):** Vulnerabilities can lead to SYN flood attacks, overwhelming the transport layer and disrupting TCP connections.

7. VBA

CVE Number: CVE-2024-23441

Publish date: 01/29/2024

CVSS 3.x Severity

Base Score: 5.5 medium

Exploitability Metrics

- **Attack Vector (AV)**: N (Network)
- **Attack Complexity (AC)**: L (Low)
- **Privileges Required (PR)**: N (None)
- **User Interaction (UI)**: Y (Required)
- **Scope (S)**: U (Unchanged)

Impact Metrics

- **Confidentiality Impact (C)**: M (Medium)
- **Integrity Impact (I)**: H (High)
- **Availability Impact (A)**: N (None)

Attack Levels

- **Low**: Minor exploitation leads to limited access to non-sensitive data.
- **Medium**: Unauthorized execution of macros, potentially accessing user data.
- **High**: Significant manipulation of application behavior, risking critical data integrity.
- **Critical**: Widespread exploitation affects multiple users, leading to major data breaches.

Impact on Computing Devices

- **User Devices**: Risk of executing malicious VBA scripts, leading to data exposure.
- **Servers**: Potential compromise of applications that rely on VBA, impacting functionality.
- **Network Infrastructure**: Minor disruptions may occur if scripts manipulate data transmission.

OSI Model Layers Affected

- **Layer 5 (Session Layer)**: This can lead to session hijacking if VBA scripts manipulate authentication tokens.
- **Layer 2 (Data Link Layer)**: This may affect data packets during local transmission if scripts manipulate network interactions.

8. Powershell

CVE Number: CVE-2024-38033

Publish date: 07/09/2024

CVSS 3.x Severity

Base Score: 7.3 high

Exploitability Metrics

- **Attack Vector (AV)**: N (Network)
- **Attack Complexity (AC)**: L (Low)
- **Privileges Required (PR)**: N (None)
- **User Interaction (UI)**: N (None)
- **Scope (S)**: U (Unchanged)

Impact Metrics

- **Confidentiality Impact (C)**: H (High)
- **Integrity Impact (I)**: H (High)
- **Availability Impact (A)**: L (Low)

Attack Levels

- **Low**: Limited unauthorized access to non-sensitive data.
- **Medium**: Execution of unauthorized PowerShell scripts affecting user data.
- **High**: Significant data manipulation or exfiltration, risking critical information.
- **Critical**: Widespread exploitation leads to severe data breaches across multiple systems.

Impact on Computing Devices

- **User Devices**: Risk of executing malicious PowerShell commands, leading to data exposure.
- **Servers**: Compromise of server integrity and potential unauthorized access to sensitive resources.
- **Network Infrastructure**: May lead to disruptions if malicious scripts affect network operations.

OSI Model Layers Affected

- **Layer 4 (Transport Layer)**: Could manipulate data flows over TCP/UDP, affecting reliable communication.
- **Layer 3 (Network Layer)**: May exploit network protocols to carry out unauthorized data transmission.

9. BASH

CVE Number: CVE-2024-46678

Publish date: 09/13/2024

CVSS 3.x Severity

Base Score: 5.5 medium

Exploitability Metrics

- **Attack Vector (AV)**: N (Network)
- **Attack Complexity (AC)**: L (Low)
- **Privileges Required (PR)**: N (None)
- **User Interaction (UI)**: N (None)
- **Scope (S)**: U (Unchanged)

Impact Metrics

- **Confidentiality Impact (C)**: M (Medium)
- **Integrity Impact (I)**: H (High)

- **Availability Impact (A)**: N (None)

Attack Levels

- **Low**: Minimal unauthorized access to non-critical data.
- **Medium**: Execution of malicious BASH commands affecting user settings or files.
- **High**: Significant manipulation of system processes or data, risking critical operations.
- **Critical**: Widespread exploitation leads to severe disruptions or data breaches across systems.

Impact on Computing Devices

- **User Devices**: Risk of executing harmful BASH scripts, compromising user data.
- **Servers**: Potential for unauthorized access and manipulation of server configurations.
- **Network Infrastructure**: May cause disruptions in services if BASH scripts affect network functions.

OSI Model Layers Affected

- **Layer 7 (Application Layer)**: Directly affects applications and scripts that use BASH, enabling execution of harmful commands.
- **Layer 4 (Transport Layer)**: This could influence data transmission, potentially leading to unauthorized data flows.

Source: https://nvd.nist.gov/vuln-metrics/cvss