ICS vulnerability - ICS Advisory (ICSA-22-104-05) Siemens OpenSSL Vulnerabilities in Industrial Products

By: Aidan Shaughnessy, Mahish Mahendarkar, Om Tatipamula, Innocent Green

Introduction/Background

Vulnerability: NULL Pointer Dereference

Equipment/Vendor: Siemens Industrial Products

ATTENTION/RISK: Exploitable remotely/high attack complexity

Risk Evaluation: Successful exploitation of this vulnerability may allow an unauthenticated attacker to cause a denial-of-service condition if a maliciously crafted renegotiation message is sent.

Overview: An OpenSSL TLS server may crash if sent a maliciously crafted renegotiation ClientHello message from a client. If a TLSv1.2 renegotiation ClientHello omits the signature_algorithms extension, where it was present in the initial ClientHello, but includes a signature_algorithms_cert extension, then a NULL pointer dereference will occur, leading to a crash and a denial-of-service condition.

Objectives and Goals

Problem Statement: To take defensive measures to minimize the risk of exploitation of this vulnerability, by minimizing network exposure for all control system devices.

- Minimize network exposure for all control system devices and/or systems, and ensure they are not accessible from the Internet.
- Locate control system networks and remote devices behind firewalls and isolate them from the business network.
- When remote access is required, use secure methods, such as Virtual Private Networks (VPNs), recognizing VPNs may have vulnerabilities and should be updated to the most current version available. Also recognize VPN is only as secure as its connected devices.

Objective: Using software that utilizes pointers, we perform the NULL pointer exception vulnerability, by adding defensive measures and mitigations the goal is to make the application being affected not crash.

Implementation and architecture of each paper

- Digital Webpage by CISA
  - “Targeted Cyber Intrusion Detection and Mitigation Strategies”
- CWE-476 Entry from MITRE
  - Encyclopedia of common vulnerabilities
- Research paper
  - Seven Pernicious Kingdoms
- Web article on CWE-476
  - ImmuniWeb
  - (͡° ͜ʖ ͡°)

Challenges Addressed

- CISA
  - Recommended practices
  - Examples: Credential management, network segmentation, RBAC, Whitelisting, etc.
- MITRE
  - Relations to other CWE, Platforms, Examples, Observed CVEs
- Seven Pernicious Kingdoms
  - Taxonomy of Software Security Errors (7+1 Kingdoms)
  - Several phylum under each category
- Immuniweb
  - Description, Impact, Affected Software, Severity & CVSS Scoring, and Mitigations

Mitigation strategies

Implementation : Check the results of all functions that return a value and verify that the value is non-null before acting upon it.

Requirements: The choice could be made to use a language that is not susceptible to these issues.

Architecture and Design : Identify all variables and data stores that receive information from external sources, and apply input validation to make sure that they are only initialized to expected values.

Testing : Use automated static analysis tools that target this type of weakness.

Automated Dynamic Analysis: This weakness can be detected using dynamic tools and techniques that interact with the software using large test suites with many diverse inputs

Manual Dynamic Analysis : Identify error conditions that are not likely to occur during normal usage and trigger them

Notes on Credential Management and Logging Capabilities

- Permission Management
  - Hierarchical privileges
  - Risk assessment prior to admin control over own systems
  - Restrict SeDebugPrivilege (DLL vuln)
- Network/System design
  - Internet/DMZ/intranet
  - Baseline image potential risk (shared password local machines)
  - Reboot after privileged user usage
  - No LAN Manager hash(legacy consideration)
  - MFA(smart cards/regular password updates)

- Logging Capabilities
  - Firewall, proxy,DNS,IDS,packet captures, flow data from routers/switches, host and application logs
- Secure Practices
  - DNS Logging with Host Level Granularity (malware uses domain name based C2, historical view)
  - Audit Network Hosts for Suspicious Files (MD5 hash check for known signatures across enterprise hosts)
  - Network Segmentation
  - RBAC
  - Whitelisting Applications

Reflection

Best Practice Takeaway

- Operational guidelines for industrial security
- Minimizing network exposure for control system devices/ensuring non access via internet
- Control system networks and remote devices behind firewalls/isolated from business networks
- VPN only as secure as connected devices
- Impact Analysis
- Risk Assessment precedes defensive measures

Sources

Targeted cyber intrusion detection and mitigation strategies (update B). CISA. (n.d.). Retrieved April 21, 2022, from https://www.cisa.gov/uscert/ics/tips/ICS-TIP-12-146-01B

Common weakness enumeration. CWE. (n.d.). Retrieved April 21, 2022, from https://cwe.mitre.org/data/definitions/476.html

Seven pernicious kingdoms: A taxonomy of ... - samate | NIST. (n.d.). Retrieved April 22, 2022, from https://samate.nist.gov/SSATTM_Content/papers/Seven%20Pernicious%20Kingdoms%20-%20Taxonomy%20of%20Sw%20Security%20Errors%20-%20Tsipenyuk%20-%20Chess%20-%20McGraw.pdf

NULL pointer dereference vulnerability: CWE-476 weakness: Exploitation and remediation. ImmuniWeb. (n.d.). Retrieved April 21, 2022, from https://www.immuniweb.com/vulnerability/null-pointer-dereference.html#severity