QuickTARA Security Analysis Report

Components Analysis

Component: Engine Control Unit

Type: ECU
Safety Level: ASIL D
Interfaces: CAN, FlexRay
Access Points: Debug Port, OBD-II
Data Types: Configuration, Sensor Data, Control Commands
Location: Internal
Trust Zone: Critical
Connected To: ECU003, SNS001, ECU002

Identified Threats:

- Accessing Functionality Not Properly Constrained by ACLs
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5
  Risk Scores: Financial: 3.2, Safety: 3.2, Privacy: 16.0
  Risk Factors: exposure: 0.50, complexity: 0.70, attack_surface: 1.00
  Description: In applications, particularly web applications, access to functionality is mitigated by an authorization framework. This framework maps Access Control Lists (ACLs) to elements of the application's fun...

- Buffer Overflow via Environment Variables
  Impact Scores: Financial: 5, Safety: 1, Privacy: 1
  Risk Scores: Financial: 16.0, Safety: 3.2, Privacy: 3.2
  Risk Factors: exposure: 0.50, complexity: 0.70, attack_surface: 1.00
  Description: This attack pattern involves causing a buffer overflow through manipulation of environment variables. Once the adversary finds that they can modify an environment variable, they may try to overflow as...

- Server Side Include (SSI) Injection
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5
  Risk Scores: Financial: 3.2, Safety: 3.2, Privacy: 16.0
  Risk Factors: exposure: 0.50, complexity: 0.70, attack_surface: 1.00
  Description: An attacker can use Server Side Include (SSI) Injection to send code to a web application that then gets executed by the web server. Doing so enables the attacker to achieve similar results to Cross S...

- Buffer Manipulation
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5
  Risk Scores: Financial: 3.2, Safety: 3.2, Privacy: 16.0
  Risk Factors: exposure: 0.50, complexity: 0.70, attack_surface: 1.00
  Description: An adversary manipulates an application's interaction with a buffer in an attempt to read or modify data they shouldn't have access to. Buffer attacks are distinguished in that it is the buffer space ...

- Format String Injection
  Impact Scores: Financial: 1, Safety: 2.8, Privacy: 5
  Risk Scores: Financial: 3.2, Safety: 8.959999999999999, Privacy: 16.0
  Risk Factors: exposure: 0.50, complexity: 0.70, attack_surface: 1.00
  Description: An adversary includes formatting characters in a string input field on the target application. Most

applications assume that users will provide static text and may respond unpredictably to the presenc...

- Cache Poisoning
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5
  Risk Scores: Financial: 3.2, Safety: 3.2, Privacy: 16.0
  Risk Factors: exposure: 0.50, complexity: 0.70, attack_surface: 1.00
  Description: An attacker exploits the functionality of cache technologies to cause specific data to be cached that aids the attackers' objectives. This describes any attack whereby an attacker places incorrect or ...

- DNS Cache Poisoning
  Impact Scores: Financial: 5, Safety: 1, Privacy: 1
  Risk Scores: Financial: 16.0, Safety: 3.2, Privacy: 3.2
  Risk Factors: exposure: 0.50, complexity: 0.70, attack_surface: 1.00
  Description: A domain name server translates a domain name (such as www.example.com) into an IP address that Internet hosts use to contact Internet resources. An adversary modifies a public DNS cache to cause cert...

- Command Delimiters
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5
  Risk Scores: Financial: 3.2, Safety: 3.2, Privacy: 16.0
  Risk Factors: exposure: 0.50, complexity: 0.70, attack_surface: 1.00
  Description: An attack of this type exploits a programs' vulnerabilities that allows an attacker's commands to be concatenated onto a legitimate command with the intent of targeting other resources such as the fil...

- Redirect Access to Libraries
  Impact Scores: Financial: 1, Safety: 5, Privacy: 1
  Risk Scores: Financial: 3.2, Safety: 16.0, Privacy: 3.2
  Risk Factors: exposure: 0.50, complexity: 0.70, attack_surface: 1.00
  Description: An adversary exploits a weakness in the way an application searches for external libraries to manipulate the execution flow to point to an adversary supplied library or code base. This pattern of atta...

- Using Malicious Files
  Impact Scores: Financial: 5, Safety: 1, Privacy: 1
  Risk Scores: Financial: 16.0, Safety: 3.2, Privacy: 3.2
  Risk Factors: exposure: 0.50, complexity: 0.70, attack_surface: 1.00
  Description: An attack of this type exploits a system's configuration that allows an adversary to either directly access an executable file, for example through shell access; or in a possible worst case allows an ...

- XSS Targeting Non-Script Elements
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5
  Risk Scores: Financial: 3.2, Safety: 3.2, Privacy: 16.0
  Risk Factors: exposure: 0.50, complexity: 0.70, attack_surface: 1.00
  Description: This attack is a form of Cross-Site Scripting (XSS) where malicious scripts are embedded in elements that are not expected to host scripts such as image tags (<img>), comments in XML documents (< !-CD...

- Malicious Automated Software Update via Redirection
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5
  Risk Scores: Financial: 3.2, Safety: 3.2, Privacy: 16.0
  Risk Factors: exposure: 0.50, complexity: 0.70, attack_surface: 1.00
  Description: An attacker exploits two layers of weaknesses in server or client software for automated update mechanisms to undermine the integrity of the target code-base. The first weakness involves a failure to ...

- PHP Remote File Inclusion
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5

Risk Scores: Financial: 3.2, Safety: 3.2, Privacy: 16.0
Risk Factors: exposure: 0.50, complexity: 0.70, attack_surface: 1.00
Description: In this pattern the adversary is able to load and execute arbitrary code remotely available from the application. This is usually accomplished through an insecurely configured PHP runtime environment ...

- XSS Using Alternate Syntax
Impact Scores: Financial: 1, Safety: 1, Privacy: 5
Risk Scores: Financial: 3.2, Safety: 3.2, Privacy: 16.0
Risk Factors: exposure: 0.50, complexity: 0.70, attack_surface: 1.00
Description: An adversary uses alternate forms of keywords or commands that result in the same action as the primary form but which may not be caught by filters. For example, many keywords are processed in a case ...

- Serialized Data External Linking
Impact Scores: Financial: 1, Safety: 1, Privacy: 5
Risk Scores: Financial: 3.2, Safety: 3.2, Privacy: 16.0
Risk Factors: exposure: 0.50, complexity: 0.70, attack_surface: 1.00
Description: An adversary creates a serialized data file (e.g. XML, YAML, etc...) that contains an external data reference. Because serialized data parsers may not validate documents with external references, ther...

- Serialized Data Parameter Blowup
Impact Scores: Financial: 1, Safety: 1, Privacy: 5
Risk Scores: Financial: 3.2, Safety: 3.2, Privacy: 16.0
Risk Factors: exposure: 0.50, complexity: 0.70, attack_surface: 1.00
Description: This attack exploits certain serialized data parsers (e.g., XML, YAML, etc.) which manage data in an inefficient manner. The attacker crafts an serialized data file with multiple configuration paramet...

- Leveraging Race Conditions
Impact Scores: Financial: 5, Safety: 1, Privacy: 1
Risk Scores: Financial: 16.0, Safety: 3.2, Privacy: 3.2
Risk Factors: exposure: 0.50, complexity: 0.70, attack_surface: 1.00
Description: The adversary targets a race condition occurring when multiple processes access and manipulate the same resource concurrently, and the outcome of the execution depends on the particular order in which...

- Leveraging Time-of-Check and Time-of-Use (TOCTOU) Race Conditions
Impact Scores: Financial: 5, Safety: 1, Privacy: 1
Risk Scores: Financial: 16.0, Safety: 3.2, Privacy: 3.2
Risk Factors: exposure: 0.50, complexity: 0.70, attack_surface: 1.00
Description: This attack targets a race condition occurring between the time of check (state) for a resource and the time of use of a resource. A typical example is file access. The adversary can leverage a file a...

- Leverage Executable Code in Non-Executable Files
Impact Scores: Financial: 5, Safety: 1, Privacy: 1
Risk Scores: Financial: 16.0, Safety: 3.2, Privacy: 3.2
Risk Factors: exposure: 0.50, complexity: 0.70, attack_surface: 1.00
Description: An attack of this type exploits a system's trust in configuration and resource files. When the executable loads the resource (such as an image file or configuration file) the attacker has modified the...

- Retrieve Embedded Sensitive Data
Impact Scores: Financial: 1, Safety: 1, Privacy: 5
Risk Scores: Financial: 3.2, Safety: 3.2, Privacy: 16.0
Risk Factors: exposure: 0.50, complexity: 0.70, attack_surface: 1.00
Description: An attacker examines a target system to find sensitive data that has been embedded within it. This information can reveal confidential contents, such as account numbers or individual keys/credentials ...

- Leveraging/Manipulating Configuration File Search Paths
  Impact Scores: Financial: 5, Safety: 1, Privacy: 1
  Risk Scores: Financial: 16.0, Safety: 3.2, Privacy: 3.2
  Risk Factors: exposure: 0.50, complexity: 0.70, attack_surface: 1.00
  Description: This pattern of attack sees an adversary load a malicious resource into a program's standard path so that when a known command is executed then the system instead executes the malicious component. The...

- Manipulating Writeable Terminal Devices
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5
  Risk Scores: Financial: 3.2, Safety: 3.2, Privacy: 16.0
  Risk Factors: exposure: 0.50, complexity: 0.70, attack_surface: 1.00
  Description: This attack exploits terminal devices that allow themselves to be written to by other users. The attacker sends command strings to the target terminal device hoping that the target user will hit enter...

- Using Meta-characters in E-mail Headers to Inject Malicious Payloads
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5
  Risk Scores: Financial: 3.2, Safety: 3.2, Privacy: 16.0
  Risk Factors: exposure: 0.50, complexity: 0.70, attack_surface: 1.00
  Description: This type of attack involves an attacker leveraging meta-characters in email headers to inject improper behavior into email programs. Email software has become increasingly sophisticated and feature-r...

- Overflow Binary Resource File
  Impact Scores: Financial: 5, Safety: 1, Privacy: 1
  Risk Scores: Financial: 16.0, Safety: 3.2, Privacy: 3.2
  Risk Factors: exposure: 0.50, complexity: 0.70, attack_surface: 1.00
  Description: An attack of this type exploits a buffer overflow vulnerability in the handling of binary resources. Binary resources may include music files like MP3, image files like JPEG files, and any other binar...

- Buffer Overflow via Symbolic Links
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5
  Risk Scores: Financial: 3.2, Safety: 3.2, Privacy: 16.0
  Risk Factors: exposure: 0.50, complexity: 0.70, attack_surface: 1.00
  Description: This type of attack leverages the use of symbolic links to cause buffer overflows. An adversary can try to create or manipulate a symbolic link file such that its contents result in out of bounds data...

- Overflow Variables and Tags
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5
  Risk Scores: Financial: 3.2, Safety: 3.2, Privacy: 16.0
  Risk Factors: exposure: 0.50, complexity: 0.70, attack_surface: 1.00
  Description: This type of attack leverages the use of tags or variables from a formatted configuration data to cause buffer overflow. The adversary crafts a malicious HTML page or configuration file that includes ...

- Passing Local Filenames to Functions That Expect a URL
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5
  Risk Scores: Financial: 3.2, Safety: 3.2, Privacy: 16.0
  Risk Factors: exposure: 0.50, complexity: 0.70, attack_surface: 1.00
  Description: This attack relies on client side code to access local files and resources instead of URLs. When the client browser is expecting a URL string, but instead receives a request for a local file, that exe...

- Poison Web Service Registry
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5
  Risk Scores: Financial: 3.2, Safety: 3.2, Privacy: 16.0
  Risk Factors: exposure: 0.50, complexity: 0.70, attack_surface: 1.00

Description: SOA and Web Services often use a registry to perform look up, get schema information, and metadata about services. A poisoned registry can redirect (think phishing for servers) the service requester t...

- Session Credential Falsification through Prediction
  Impact Scores: Financial: 5, Safety: 1, Privacy: 1
  Risk Scores: Financial: 16.0, Safety: 3.2, Privacy: 3.2
  Risk Factors: exposure: 0.50, complexity: 0.70, attack_surface: 1.00
  Description: This attack targets predictable session ID in order to gain privileges. The attacker can predict the session ID used during a transaction to perform spoofing and session hijacking....

- Using Slashes and URL Encoding Combined to Bypass Validation Logic
  Impact Scores: Financial: 5, Safety: 1, Privacy: 1
  Risk Scores: Financial: 16.0, Safety: 3.2, Privacy: 3.2
  Risk Factors: exposure: 0.50, complexity: 0.70, attack_surface: 1.00
  Description: This attack targets the encoding of the URL combined with the encoding of the slash characters. An attacker can take advantage of the multiple ways of encoding a URL and abuse the interpretation of th...

- Avoid Security Tool Identification by Adding Data
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5
  Risk Scores: Financial: 3.2, Safety: 3.2, Privacy: 16.0
  Risk Factors: exposure: 0.50, complexity: 0.70, attack_surface: 1.00
  Description: An adversary adds data to a file to increase the file size beyond what security tools are capable of handling in an attempt to mask their actions. In addition to this, adding data to a file also chang...

- Voice Phishing
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5
  Risk Scores: Financial: 3.2, Safety: 3.2, Privacy: 16.0
  Risk Factors: exposure: 0.50, complexity: 0.70, attack_surface: 1.00
  Description: An adversary targets users with a phishing attack for the purpose of soliciting account passwords or sensitive information from the user. Voice Phishing is a variation of the Phishing social engineeri...

- Malicious Automated Software Update via Spoofing
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5
  Risk Scores: Financial: 3.2, Safety: 3.2, Privacy: 16.0
  Risk Factors: exposure: 0.50, complexity: 0.70, attack_surface: 1.00
  Description: An attackers uses identify or content spoofing to trick a client into performing an automated software update from a malicious source. A malicious automated software update that leverages spoofing can...

- String Format Overflow in syslog()
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5
  Risk Scores: Financial: 3.2, Safety: 3.2, Privacy: 16.0
  Risk Factors: exposure: 0.50, complexity: 0.70, attack_surface: 1.00
  Description: This attack targets applications and software that uses the syslog() function insecurely. If an application does not explicitely use a format string parameter in a call to syslog(), user input can be ...

- Blind SQL Injection
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5
  Risk Scores: Financial: 3.2, Safety: 3.2, Privacy: 16.0
  Risk Factors: exposure: 0.50, complexity: 0.70, attack_surface: 1.00
  Description: Blind SQL Injection results from an insufficient mitigation for SQL Injection. Although suppressing database error messages are considered best practice, the suppression alone is not sufficient to pre...

- URL Encoding

Impact Scores: Financial: 5, Safety: 1, Privacy: 1
Risk Scores: Financial: 16.0, Safety: 3.2, Privacy: 3.2
Risk Factors: exposure: 0.50, complexity: 0.70, attack_surface: 1.00
Description: This attack targets the encoding of the URL. An adversary can take advantage of the multiple way of encoding an URL and abuse the interpretation of the URL....

- User-Controlled Filename
Impact Scores: Financial: 1, Safety: 1, Privacy: 5
Risk Scores: Financial: 3.2, Safety: 3.2, Privacy: 16.0
Risk Factors: exposure: 0.50, complexity: 0.70, attack_surface: 1.00
Description: An attack of this type involves an adversary inserting malicious characters (such as a XSS redirection) into a filename, directly or indirectly that is then used by the target software to generate HTM...

- Manipulating User-Controlled Variables
Impact Scores: Financial: 2.8, Safety: 1, Privacy: 5
Risk Scores: Financial: 8.959999999999999, Safety: 3.2, Privacy: 16.0
Risk Factors: exposure: 0.50, complexity: 0.70, attack_surface: 1.00
Description: This attack targets user controlled variables (DEBUG=1, PHP Globals, and So Forth). An adversary can override variables leveraging user-supplied, untrusted query variables directly used on the applica...

- Using Escaped Slashes in Alternate Encoding
Impact Scores: Financial: 5, Safety: 1, Privacy: 1
Risk Scores: Financial: 16.0, Safety: 3.2, Privacy: 3.2
Risk Factors: exposure: 0.50, complexity: 0.70, attack_surface: 1.00
Description: This attack targets the use of the backslash in alternate encoding. An adversary can provide a backslash as a leading character and causes a parser to believe that the next character is special. This ...

- Buffer Overflow in an API Call
Impact Scores: Financial: 5, Safety: 1, Privacy: 1
Risk Scores: Financial: 16.0, Safety: 3.2, Privacy: 3.2
Risk Factors: exposure: 0.50, complexity: 0.70, attack_surface: 1.00
Description: This attack targets libraries or shared code modules which are vulnerable to buffer overflow attacks. An adversary who has knowledge of known vulnerable libraries or shared code can easily target soft...

- Using UTF-8 Encoding to Bypass Validation Logic
Impact Scores: Financial: 1, Safety: 5, Privacy: 1
Risk Scores: Financial: 3.2, Safety: 16.0, Privacy: 3.2
Risk Factors: exposure: 0.50, complexity: 0.70, attack_surface: 1.00
Description: This attack is a specific variation on leveraging alternate encodings to bypass validation logic. This attack leverages the possibility to encode potentially harmful input in UTF-8 and submit it to ap...

- XPath Injection
Impact Scores: Financial: 1, Safety: 1, Privacy: 5
Risk Scores: Financial: 3.2, Safety: 3.2, Privacy: 16.0
Risk Factors: exposure: 0.50, complexity: 0.70, attack_surface: 1.00
Description: An attacker can craft special user-controllable input consisting of XPath expressions to inject the XML database and bypass authentication or glean information that they normally would not be able to....

- XQuery Injection
Impact Scores: Financial: 1, Safety: 1, Privacy: 5
Risk Scores: Financial: 3.2, Safety: 3.2, Privacy: 16.0
Risk Factors: exposure: 0.50, complexity: 0.70, attack_surface: 1.00
Description: This attack utilizes XQuery to probe and attack server systems; in a similar manner that SQL Injection

allows an attacker to exploit SQL calls to RDBMS, XQuery Injection uses improperly validated data...

- OS Command Injection
  Impact Scores: Financial: 5, Safety: 1, Privacy: 1
  Risk Scores: Financial: 16.0, Safety: 3.2, Privacy: 3.2
  Risk Factors: exposure: 0.50, complexity: 0.70, attack_surface: 1.00
  Description: In this type of an attack, an adversary injects operating system commands into existing application functions. An application that uses untrusted input to build command strings is vulnerable. An adver...

- Pharming
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5
  Risk Scores: Financial: 3.2, Safety: 3.2, Privacy: 16.0
  Risk Factors: exposure: 0.50, complexity: 0.70, attack_surface: 1.00
  Description: A pharming attack occurs when the victim is fooled into entering sensitive data into supposedly trusted locations, such as an online bank site or a trading platform. An attacker can impersonate these ...

- Buffer Overflow in Local Command-Line Utilities
  Impact Scores: Financial: 5, Safety: 1, Privacy: 1
  Risk Scores: Financial: 16.0, Safety: 3.2, Privacy: 3.2
  Risk Factors: exposure: 0.50, complexity: 0.70, attack_surface: 1.00
  Description: This attack targets command-line utilities available in a number of shells. An adversary can leverage a vulnerability found in a command-line utility to escalate privilege to root....

- Reflection Attack in Authentication Protocol
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5
  Risk Scores: Financial: 3.2, Safety: 3.2, Privacy: 16.0
  Risk Factors: exposure: 0.50, complexity: 0.70, attack_surface: 1.00
  Description: An adversary can abuse an authentication protocol susceptible to reflection attack in order to defeat it. Doing so allows the adversary illegitimate access to the target system, without possessing the...

- Forced Integer Overflow
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5
  Risk Scores: Financial: 3.2, Safety: 3.2, Privacy: 16.0
  Risk Factors: exposure: 0.50, complexity: 0.70, attack_surface: 1.00
  Description: This attack forces an integer variable to go out of range. The integer variable is often used as an offset such as size of memory allocation or similarly. The attacker would typically control the valu...

- WSDL Scanning
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5
  Risk Scores: Financial: 3.2, Safety: 3.2, Privacy: 16.0
  Risk Factors: exposure: 0.50, complexity: 0.70, attack_surface: 1.00
  Description: This attack targets the WSDL interface made available by a web service. The attacker may scan the WSDL interface to reveal sensitive information about invocation patterns, underlying technology implem...

- Phishing
  Impact Scores: Financial: 1.4, Safety: 1, Privacy: 5
  Risk Scores: Financial: 4.4799999999999995, Safety: 3.2, Privacy: 16.0
  Risk Factors: exposure: 0.50, complexity: 0.70, attack_surface: 1.00
  Description: Phishing is a social engineering technique where an attacker masquerades as a legitimate entity with which the victim might do business in order to prompt the user to reveal some confidential informat...

- Flooding
  Impact Scores: Financial: 1, Safety: 1.4, Privacy: 4.199999999999999

Risk Scores: Financial: 3.2, Safety: 4.4799999999999995, Privacy: 13.439999999999998
Risk Factors: exposure: 0.50, complexity: 0.70, attack_surface: 1.00
Description: An adversary consumes the resources of a target by rapidly engaging in a large number of interactions with the target. This type of attack generally exposes a weakness in rate limiting or flow. When s...

- Directory Indexing
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.199999999999999
  Risk Scores: Financial: 3.2, Safety: 3.2, Privacy: 13.439999999999998
  Risk Factors: exposure: 0.50, complexity: 0.70, attack_surface: 1.00
  Description: An adversary crafts a request to a target that results in the target listing/indexing the content of a directory as output. One common method of triggering directory contents as output is to construct...

- Flash Parameter Injection
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.199999999999999
  Risk Scores: Financial: 3.2, Safety: 3.2, Privacy: 13.439999999999998
  Risk Factors: exposure: 0.50, complexity: 0.70, attack_surface: 1.00
  Description: An adversary takes advantage of improper data validation to inject malicious global parameters into a Flash file embedded within an HTML document. Flash files can leverage user-submitted data to confi...

- Exploiting Incorrectly Configured Access Control Security Levels
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.199999999999999
  Risk Scores: Financial: 3.2, Safety: 3.2, Privacy: 13.439999999999998
  Risk Factors: exposure: 0.50, complexity: 0.70, attack_surface: 1.00
  Description: An attacker exploits a weakness in the configuration of access controls and is able to bypass the intended protection that these measures guard against and thereby obtain unauthorized access to the sy...

- Exponential Data Expansion
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.199999999999999
  Risk Scores: Financial: 3.2, Safety: 3.2, Privacy: 13.439999999999998
  Risk Factors: exposure: 0.50, complexity: 0.70, attack_surface: 1.00
  Description: An adversary submits data to a target application which contains nested exponential data expansion to produce excessively large output. Many data format languages allow the definition of macro-like st...

- Inducing Account Lockout
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.199999999999999
  Risk Scores: Financial: 3.2, Safety: 3.2, Privacy: 13.439999999999998
  Risk Factors: exposure: 0.50, complexity: 0.70, attack_surface: 1.00
  Description: An attacker leverages the security functionality of the system aimed at thwarting potential attacks to launch a denial of service attack against a legitimate system user. Many systems, for instance, i...

- XML Routing Detour Attacks
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.199999999999999
  Risk Scores: Financial: 3.2, Safety: 3.2, Privacy: 13.439999999999998
  Risk Factors: exposure: 0.50, complexity: 0.70, attack_surface: 1.00
  Description: An attacker subverts an intermediate system used to process XML content and forces the intermediate to modify and/or re-route the processing of the content. XML Routing Detour Attacks are Adversary in...

- Fuzzing
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.199999999999999
  Risk Scores: Financial: 3.2, Safety: 3.2, Privacy: 13.439999999999998
  Risk Factors: exposure: 0.50, complexity: 0.70, attack_surface: 1.00
  Description: In this attack pattern, the adversary leverages fuzzing to try to identify weaknesses in the system. Fuzzing is a software security and functionality testing method that feeds randomly constructed inp...

- Manipulating Opaque Client-based Data Tokens
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.199999999999999
  Risk Scores: Financial: 3.2, Safety: 3.2, Privacy: 13.439999999999998
  Risk Factors: exposure: 0.50, complexity: 0.70, attack_surface: 1.00
  Description: In circumstances where an application holds important data client-side in tokens (cookies, URLs, data files, and so forth) that data can be manipulated. If client or server-side application components...

- CAN Injection
  Impact Scores: Financial: 4.199999999999999, Safety: 5, Privacy: 2.8
  Risk Scores: Financial: 10.08, Safety: 12.000000000000002, Privacy: 6.720000000000001
  Risk Factors: exposure: 0.50, complexity: 0.70, attack_surface: 1.00
  Description: Manipulation of CAN bus messages leading to vehicle malfunction...

- Sensor Data Manipulation
  Impact Scores: Financial: 4.199999999999999, Safety: 5, Privacy: 2.8
  Risk Scores: Financial: 10.08, Safety: 12.000000000000002, Privacy: 6.720000000000001
  Risk Factors: exposure: 0.50, complexity: 0.70, attack_surface: 1.00
  Description: Tampering with sensor data leading to incorrect vehicle behavior...

- HTTP Request Splitting
  Impact Scores: Financial: 5, Safety: 1, Privacy: 1
  Risk Scores: Financial: 12.000000000000002, Safety: 2.4000000000000004, Privacy: 2.4000000000000004
  Risk Factors: exposure: 0.50, complexity: 0.70, attack_surface: 1.00
  Description: An adversary abuses the flexibility and discrepancies in the parsing and interpretation of HTTP Request messages by different intermediary HTTP agents (e.g., load balancer, reverse proxy, web caching ...

- Serialized Data with Nested Payloads
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5
  Risk Scores: Financial: 2.4000000000000004, Safety: 2.4000000000000004, Privacy: 12.000000000000002
  Risk Factors: exposure: 0.50, complexity: 0.70, attack_surface: 1.00
  Description: Applications often need to transform data in and out of a data format (e.g., XML and YAML) by using a parser. It may be possible for an adversary to inject data that may have an adverse effect on the ...

- Command Injection
  Impact Scores: Financial: 5, Safety: 1, Privacy: 1
  Risk Scores: Financial: 12.000000000000002, Safety: 2.4000000000000004, Privacy: 2.4000000000000004
  Risk Factors: exposure: 0.50, complexity: 0.70, attack_surface: 1.00
  Description: An adversary looking to execute a command of their choosing, injects new items into an existing command thus modifying interpretation away from what was intended. Commands in this context are often st...

- Leveraging Race Conditions via Symbolic Links
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5
  Risk Scores: Financial: 2.4000000000000004, Safety: 2.4000000000000004, Privacy: 12.000000000000002
  Risk Factors: exposure: 0.50, complexity: 0.70, attack_surface: 1.00
  Description: This attack leverages the use of symbolic links (Symlinks) in order to write to sensitive files. An attacker can create a Symlink link to a target file not otherwise accessible to them. When the privi...

- HTTP Response Smuggling
  Impact Scores: Financial: 5, Safety: 1, Privacy: 1
  Risk Scores: Financial: 12.000000000000002, Safety: 2.4000000000000004, Privacy: 2.4000000000000004
  Risk Factors: exposure: 0.50, complexity: 0.70, attack_surface: 1.00
  Description: An adversary manipulates and injects malicious content in the form of secret unauthorized HTTP responses, into a single HTTP response from a vulnerable or compromised back-end HTTP agent (e.g., server...

```
- SOAP Manipulation
  Impact Scores: Financial: 5, Safety: 1, Privacy: 1
  Risk Scores: Financial: 12.000000000000002, Safety: 2.4000000000000004, Privacy: 2.4000000000000004
  Risk Factors: exposure: 0.50, complexity: 0.70, attack_surface: 1.00
  Description: Simple Object Access Protocol (SOAP) is used as a communication protocol between a client and server to invoke web services on the server. It is an XML-based protocol, and therefore suffers from many ...

- HTTP Request Smuggling
  Impact Scores: Financial: 5, Safety: 1, Privacy: 1
  Risk Scores: Financial: 12.000000000000002, Safety: 2.4000000000000004, Privacy: 2.4000000000000004
  Risk Factors: exposure: 0.50, complexity: 0.70, attack_surface: 1.00
  Description: An adversary abuses the flexibility and discrepancies in the parsing and interpretation of HTTP Request messages using various HTTP headers, request-line and body parameters as well as message sizes (...

- HTTP Response Splitting
  Impact Scores: Financial: 5, Safety: 1, Privacy: 1
  Risk Scores: Financial: 12.000000000000002, Safety: 2.4000000000000004, Privacy: 2.4000000000000004
  Risk Factors: exposure: 0.50, complexity: 0.70, attack_surface: 1.00
  Description: An adversary manipulates and injects malicious content, in the form of secret unauthorized HTTP responses, into a single HTTP response from a vulnerable or compromised back-end HTTP agent (e.g., web s...

- Using Alternative IP Address Encodings
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5
  Risk Scores: Financial: 2.4000000000000004, Safety: 2.4000000000000004, Privacy: 12.000000000000002
  Risk Factors: exposure: 0.50, complexity: 0.70, attack_surface: 1.00
  Description: This attack relies on the adversary using unexpected formats for representing IP addresses. Networked applications may expect network location information in a specific format, such as fully qualified...

- Exploiting Multiple Input Interpretation Layers
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5
  Risk Scores: Financial: 2.4000000000000004, Safety: 2.4000000000000004, Privacy: 12.000000000000002
  Risk Factors: exposure: 0.50, complexity: 0.70, attack_surface: 1.00
  Description: An attacker supplies the target software with input data that contains sequences of special characters designed to bypass input validation logic. This exploit relies on the target making multiples pas...

- Development Alteration
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5
  Risk Scores: Financial: 2.4000000000000004, Safety: 2.4000000000000004, Privacy: 12.000000000000002
  Risk Factors: exposure: 0.50, complexity: 0.70, attack_surface: 1.00
  Description: An adversary modifies a technology, product, or component during its development to acheive a negative impact once the system is deployed. The goal of the adversary is to modify the system in such a w...

- Malicious Logic Insertion into Product Software via Configuration Management Manipulation
  Impact Scores: Financial: 5, Safety: 1, Privacy: 1
  Risk Scores: Financial: 12.000000000000002, Safety: 2.4000000000000004, Privacy: 2.4000000000000004
  Risk Factors: exposure: 0.50, complexity: 0.70, attack_surface: 1.00
  Description: An adversary exploits a configuration management system so that malicious logic is inserted into a software products build, update or deployed environment. If an adversary can control the elements inc...

- Design Alteration
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5
  Risk Scores: Financial: 2.4000000000000004, Safety: 2.4000000000000004, Privacy: 12.000000000000002
  Risk Factors: exposure: 0.50, complexity: 0.70, attack_surface: 1.00
```

Description: An adversary modifies the design of a technology, product, or component to acheive a negative impact once the system is deployed. In this type of attack, the goal of the adversary is to modify the des...

- Contradictory Destinations in Traffic Routing Schemes
  Impact Scores: Financial: 5, Safety: 1, Privacy: 1
  Risk Scores: Financial: 12.000000000000002, Safety: 2.4000000000000004, Privacy: 2.4000000000000004
  Risk Factors: exposure: 0.50, complexity: 0.70, attack_surface: 1.00
  Description: Adversaries can provide contradictory destinations when sending messages. Traffic is routed in networks using the domain names in various headers available at different levels of the OSI model. In a C...

- Local Execution of Code
  Impact Scores: Financial: 5, Safety: 1, Privacy: 1
  Risk Scores: Financial: 12.000000000000002, Safety: 2.4000000000000004, Privacy: 2.4000000000000004
  Risk Factors: exposure: 0.50, complexity: 0.70, attack_surface: 1.00
  Description: An adversary installs and executes malicious code on the target system in an effort to achieve a negative technical impact. Examples include rootkits, ransomware, spyware, adware, and others....

- Object Injection
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5
  Risk Scores: Financial: 2.4000000000000004, Safety: 2.4000000000000004, Privacy: 12.000000000000002
  Risk Factors: exposure: 0.50, complexity: 0.70, attack_surface: 1.00
  Description: An adversary attempts to exploit an application by injecting additional, malicious content during its processing of serialized objects. Developers leverage serialization in order to convert data or st...

- Root/Jailbreak Detection Evasion via Debugging
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5
  Risk Scores: Financial: 2.4000000000000004, Safety: 2.4000000000000004, Privacy: 12.000000000000002
  Risk Factors: exposure: 0.50, complexity: 0.70, attack_surface: 1.00
  Description: An adversary inserts a debugger into the program entry point of a mobile application to modify the application binary, with the goal of evading Root/Jailbreak detection. Mobile device users often Root...

- Bluetooth Impersonation AttackS (BIAS)
  Impact Scores: Financial: 5, Safety: 1, Privacy: 1
  Risk Scores: Financial: 12.000000000000002, Safety: 2.4000000000000004, Privacy: 2.4000000000000004
  Risk Factors: exposure: 0.50, complexity: 0.70, attack_surface: 1.00
  Description: An adversary disguises the MAC address of their Bluetooth enabled device to one for which there exists an active and trusted connection and authenticates successfully. The adversary can then perform m...

- Alteration of a Software Update
  Impact Scores: Financial: 5, Safety: 1, Privacy: 1
  Risk Scores: Financial: 12.000000000000002, Safety: 2.4000000000000004, Privacy: 2.4000000000000004
  Risk Factors: exposure: 0.50, complexity: 0.70, attack_surface: 1.00
  Description: An adversary with access to an organization’s software update infrastructure inserts malware into the content of an outgoing update to fielded systems where a wide range of malicious effects are possi...

- Exploitation of Improperly Controlled Hardware Security Identifiers
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5
  Risk Scores: Financial: 2.4000000000000004, Safety: 2.4000000000000004, Privacy: 12.000000000000002
  Risk Factors: exposure: 0.50, complexity: 0.70, attack_surface: 1.00
  Description: An adversary takes advantage of missing or incorrectly configured security identifiers (e.g., tokens), which are used for access control within a System-on-Chip (SoC), to read/write data or execute a ...

- Eavesdropping on a Monitor

Impact Scores: Financial: 1, Safety: 1, Privacy: 5
Risk Scores: Financial: 2.4000000000000004, Safety: 2.4000000000000004, Privacy: 12.000000000000002
Risk Factors: exposure: 0.50, complexity: 0.70, attack_surface: 1.00
Description: An Adversary can eavesdrop on the content of an external monitor through the air without modifying any cable or installing software, just capturing this signal emitted by the cable or video port, with...

- Browser in the Middle (BiTM)
Impact Scores: Financial: 5, Safety: 1, Privacy: 1
Risk Scores: Financial: 12.000000000000002, Safety: 2.4000000000000004, Privacy: 2.4000000000000004
Risk Factors: exposure: 0.50, complexity: 0.70, attack_surface: 1.00
Description: An adversary exploits the inherent functionalities of a web browser, in order to establish an unnoticed remote desktop connection in the victim's browser to the adversary's system. The adversary must ...

- Manipulating State
Impact Scores: Financial: 1.4, Safety: 1, Privacy: 5
Risk Scores: Financial: 3.3600000000000003, Safety: 2.4000000000000004, Privacy: 12.000000000000002
Risk Factors: exposure: 0.50, complexity: 0.70, attack_surface: 1.00
Description: The adversary modifies state information maintained by the target software or causes a state transition in hardware. If successful, the target will use this tainted state and execute in an unintended ...

- Interface Manipulation
Impact Scores: Financial: 4.199999999999999, Safety: 1, Privacy: 1
Risk Scores: Financial: 10.08, Safety: 2.4000000000000004, Privacy: 2.4000000000000004
Risk Factors: exposure: 0.50, complexity: 0.70, attack_surface: 1.00
Description: An adversary manipulates the use or processing of an interface (e.g. Application Programming Interface (API) or System-on-Chip (SoC)) resulting in an adverse impact upon the security of the system imp...

- Parameter Injection
Impact Scores: Financial: 1, Safety: 1, Privacy: 4.199999999999999
Risk Scores: Financial: 2.4000000000000004, Safety: 2.4000000000000004, Privacy: 10.08
Risk Factors: exposure: 0.50, complexity: 0.70, attack_surface: 1.00
Description: An adversary manipulates the content of request parameters for the purpose of undermining the security of the target. Some parameter encodings use text characters as separators. For example, parameter...

- Content Spoofing
Impact Scores: Financial: 4.199999999999999, Safety: 1, Privacy: 4.199999999999999
Risk Scores: Financial: 10.08, Safety: 2.4000000000000004, Privacy: 10.08
Risk Factors: exposure: 0.50, complexity: 0.70, attack_surface: 1.00
Description: An adversary modifies content to make it contain something other than what the original content producer intended while keeping the apparent source of the content unchanged. The term content spoofing ...

- Resource Location Spoofing
Impact Scores: Financial: 1, Safety: 1, Privacy: 4.199999999999999
Risk Scores: Financial: 2.4000000000000004, Safety: 2.4000000000000004, Privacy: 10.08
Risk Factors: exposure: 0.50, complexity: 0.70, attack_surface: 1.00
Description: An adversary deceives an application or user and convinces them to request a resource from an unintended location. By spoofing the location, the adversary can cause an alternate resource to be used, o...

- Cross-Site Flashing
Impact Scores: Financial: 4.199999999999999, Safety: 1, Privacy: 1
Risk Scores: Financial: 10.08, Safety: 2.4000000000000004, Privacy: 2.4000000000000004
Risk Factors: exposure: 0.50, complexity: 0.70, attack_surface: 1.00
Description: An attacker is able to trick the victim into executing a Flash document that passes commands or calls to a

Flash player browser plugin, allowing the attacker to exploit native Flash functionality in t...

- Modification of Registry Run Keys
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.199999999999999
  Risk Scores: Financial: 2.4000000000000004, Safety: 2.4000000000000004, Privacy: 10.08
  Risk Factors: exposure: 0.50, complexity: 0.70, attack_surface: 1.00
  Description: An adversary adds a new entry to the run keys in the Windows registry so that an application of their choosing is executed when a user logs in. In this way, the adversary can get their executable to o...

- Using Leading 'Ghost' Character Sequences to Bypass Input Filters
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.199999999999999
  Risk Scores: Financial: 2.4000000000000004, Safety: 2.4000000000000004, Privacy: 10.08
  Risk Factors: exposure: 0.50, complexity: 0.70, attack_surface: 1.00
  Description: Some APIs will strip certain leading characters from a string of parameters. An adversary can intentionally introduce leading ghost characters (extra characters that don't affect the validity of the r...

- Manipulate Human Behavior
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.199999999999999
  Risk Scores: Financial: 2.4000000000000004, Safety: 2.4000000000000004, Privacy: 10.08
  Risk Factors: exposure: 0.50, complexity: 0.70, attack_surface: 1.00
  Description: An adversary exploits inherent human psychological predisposition to influence a targeted individual or group to solicit information or manipulate the target into performing an action that serves the ...

- Malware-Directed Internal Reconnaissance
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.199999999999999
  Risk Scores: Financial: 2.4000000000000004, Safety: 2.4000000000000004, Privacy: 10.08
  Risk Factors: exposure: 0.50, complexity: 0.70, attack_surface: 1.00
  Description: Adversary uses malware or a similarly controlled application installed inside an organizational perimeter to gather information about the composition, configuration, and security mechanisms of a targe...

- Disable Security Software
  Impact Scores: Financial: 4.199999999999999, Safety: 1, Privacy: 1
  Risk Scores: Financial: 10.08, Safety: 2.4000000000000004, Privacy: 2.4000000000000004
  Risk Factors: exposure: 0.50, complexity: 0.70, attack_surface: 1.00
  Description: An adversary exploits a weakness in access control to disable security tools so that detection does not occur. This can take the form of killing processes, deleting registry keys so that tools do not ...

- Collect Data from Registries
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.199999999999999
  Risk Scores: Financial: 2.4000000000000004, Safety: 2.4000000000000004, Privacy: 10.08
  Risk Factors: exposure: 0.50, complexity: 0.70, attack_surface: 1.00
  Description: An adversary exploits a weakness in authorization to gather system-specific data and sensitive information within a registry (e.g., Windows Registry, Mac plist). These contain information about the sy...

- Collect Data from Screen Capture
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.199999999999999
  Risk Scores: Financial: 2.4000000000000004, Safety: 2.4000000000000004, Privacy: 10.08
  Risk Factors: exposure: 0.50, complexity: 0.70, attack_surface: 1.00
  Description: An adversary gathers sensitive information by exploiting the system's screen capture functionality. Through screenshots, the adversary aims to see what happens on the screen over the course of an oper...

- Retrieve Data from Decommissioned Devices
  Impact Scores: Financial: 1, Safety: 1.4, Privacy: 4.199999999999999

Risk Scores: Financial: 2.4000000000000004, Safety: 3.3600000000000003, Privacy: 10.08
Risk Factors: exposure: 0.50, complexity: 0.70, attack_surface: 1.00
Description: An adversary obtains decommissioned, recycled, or discarded systems and devices that can include an organization’s intellectual property, employee data, and other types of controlled information. Syst...

- Web Application Fingerprinting
  Impact Scores: Financial: 1, Safety: 1, Privacy: 2.8
  Risk Scores: Financial: 3.2, Safety: 3.2, Privacy: 8.959999999999999
  Risk Factors: exposure: 0.50, complexity: 0.70, attack_surface: 1.00
  Description: An attacker sends a series of probes to a web application in order to elicit version-dependent and type-dependent behavior that assists in identifying the target. An attacker could learn information s...

- Fuzzing for application mapping
  Impact Scores: Financial: 1, Safety: 2.8, Privacy: 1
  Risk Scores: Financial: 3.2, Safety: 8.959999999999999, Privacy: 3.2
  Risk Factors: exposure: 0.50, complexity: 0.70, attack_surface: 1.00
  Description: An attacker sends random, malformed, or otherwise unexpected messages to a target application and observes the application's log or error messages returned. The attacker does not initially know how a ...

- AJAX Footprinting
  Impact Scores: Financial: 1, Safety: 1, Privacy: 2.8
  Risk Scores: Financial: 3.2, Safety: 3.2, Privacy: 8.959999999999999
  Risk Factors: exposure: 0.50, complexity: 0.70, attack_surface: 1.00
  Description: This attack utilizes the frequent client-server roundtrips in Ajax conversation to scan a system. While Ajax does not open up new vulnerabilities per se, it does optimize them from an attacker point o...

- ECU Firmware Tampering
  Impact Scores: Financial: 5, Safety: 5, Privacy: 4.199999999999999
  Risk Scores: Financial: 8.0, Safety: 8.0, Privacy: 6.719999999999999
  Risk Factors: exposure: 0.50, complexity: 0.70, attack_surface: 1.00
  Description: Unauthorized modification of ECU firmware causing safety issues...

- Command Line Execution through SQL Injection
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5
  Risk Scores: Financial: 1.6, Safety: 1.6, Privacy: 8.0
  Risk Factors: exposure: 0.50, complexity: 0.70, attack_surface: 1.00
  Description: An attacker uses standard SQL injection methods to inject data into the command line for execution. This could be done directly through misuse of directives such as MSSQL_xp_cmdshell or indirectly thr...

- Escaping a Sandbox by Calling Code in Another Language
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5
  Risk Scores: Financial: 1.6, Safety: 1.6, Privacy: 8.0
  Risk Factors: exposure: 0.50, complexity: 0.70, attack_surface: 1.00
  Description: The attacker may submit malicious code of another language to obtain access to privileges that were not intentionally exposed by the sandbox, thus escaping the sandbox. For instance, Java code cannot ...

- Forced Deadlock
  Impact Scores: Financial: 5, Safety: 1, Privacy: 1
  Risk Scores: Financial: 8.0, Safety: 1.6, Privacy: 1.6
  Risk Factors: exposure: 0.50, complexity: 0.70, attack_surface: 1.00
  Description: The adversary triggers and exploits a deadlock condition in the target software to cause a denial of service. A deadlock can occur when two or more competing actions are waiting for each other to fini...

- Schema Poisoning
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5
  Risk Scores: Financial: 1.6, Safety: 1.6, Privacy: 8.0
  Risk Factors: exposure: 0.50, complexity: 0.70, attack_surface: 1.00
  Description: An adversary corrupts or modifies the content of a schema for the purpose of undermining the security of the target. Schemas provide the structure and content definitions for resources used by an appl...

- Hijacking a Privileged Thread of Execution
  Impact Scores: Financial: 5, Safety: 1, Privacy: 1
  Risk Scores: Financial: 8.0, Safety: 1.6, Privacy: 1.6
  Risk Factors: exposure: 0.50, complexity: 0.70, attack_surface: 1.00
  Description: An adversary hijacks a privileged thread of execution by injecting malicious code into a running process. By using a privleged thread to do their bidding, adversaries can evade process-based detection...

- USB Memory Attacks
  Impact Scores: Financial: 2.8, Safety: 1, Privacy: 5
  Risk Scores: Financial: 4.4799999999999995, Safety: 1.6, Privacy: 8.0
  Risk Factors: exposure: 0.50, complexity: 0.70, attack_surface: 1.00
  Description: An adversary loads malicious code onto a USB memory stick in order to infect any system which the device is plugged in to. USB drives present a significant security risk for business and government ag...

- Signature Spoofing by Misrepresentation
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5
  Risk Scores: Financial: 1.6, Safety: 1.6, Privacy: 8.0
  Risk Factors: exposure: 0.50, complexity: 0.70, attack_surface: 1.00
  Description: An attacker exploits a weakness in the parsing or display code of the recipient software to generate a data blob containing a supposedly valid signature, but the signer's identity is falsely represent...

- Hardware Component Substitution During Baselining
  Impact Scores: Financial: 5, Safety: 1, Privacy: 1
  Risk Scores: Financial: 8.0, Safety: 1.6, Privacy: 1.6
  Risk Factors: exposure: 0.50, complexity: 0.70, attack_surface: 1.00
  Description: An adversary with access to system components during allocated baseline development can substitute a maliciously altered hardware component for a baseline component during the product development and ...

- Malicious Hardware Update
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5
  Risk Scores: Financial: 1.6, Safety: 1.6, Privacy: 8.0
  Risk Factors: exposure: 0.50, complexity: 0.70, attack_surface: 1.00
  Description: An adversary introduces malicious hardware during an update or replacement procedure, allowing for additional compromise or site disruption at the victim location. After deployment, it is not uncommon...

- Data Injected During Configuration
  Impact Scores: Financial: 1, Safety: 5, Privacy: 5
  Risk Scores: Financial: 1.6, Safety: 8.0, Privacy: 8.0
  Risk Factors: exposure: 0.50, complexity: 0.70, attack_surface: 1.00
  Description: An attacker with access to data files and processes on a victim's system injects malicious data into critical operational data during configuration or recalibration, causing the victim's system to per...

- Open-Source Library Manipulation
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5
  Risk Scores: Financial: 1.6, Safety: 1.6, Privacy: 8.0
  Risk Factors: exposure: 0.50, complexity: 0.70, attack_surface: 1.00

Description: Adversaries implant malicious code in open source software (OSS) libraries to have it widely distributed, as OSS is commonly downloaded by developers and other users to incorporate into software devel...

- ASIC With Malicious Functionality
  Impact Scores: Financial: 5, Safety: 1, Privacy: 1
  Risk Scores: Financial: 8.0, Safety: 1.6, Privacy: 1.6
  Risk Factors: exposure: 0.50, complexity: 0.70, attack_surface: 1.00
  Description: An attacker with access to the development environment process of an application-specific integrated circuit (ASIC) for a victim system being developed or maintained after initial deployment can inser...

- Replace Trusted Executable
  Impact Scores: Financial: 5, Safety: 1, Privacy: 1
  Risk Scores: Financial: 8.0, Safety: 1.6, Privacy: 1.6
  Risk Factors: exposure: 0.50, complexity: 0.70, attack_surface: 1.00
  Description: An adversary exploits weaknesses in privilege management or access control to replace a trusted executable with a malicious version and enable the execution of malware when that trusted executable is ...

- Hardware Fault Injection
  Impact Scores: Financial: 1, Safety: 5, Privacy: 5
  Risk Scores: Financial: 1.6, Safety: 8.0, Privacy: 8.0
  Risk Factors: exposure: 0.50, complexity: 0.70, attack_surface: 1.00
  Description: The adversary uses disruptive signals or events, or alters the physical environment a device operates in, to cause faulty behavior in electronic devices. This can include electromagnetic pulses, laser...

- Carry-Off GPS Attack
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5
  Risk Scores: Financial: 1.6, Safety: 1.6, Privacy: 8.0
  Risk Factors: exposure: 0.50, complexity: 0.70, attack_surface: 1.00
  Description: A common form of a GPS spoofing attack, commonly termed a carry-off attack begins with an adversary broadcasting signals synchronized with the genuine signals observed by the target receiver. The powe...

- DLL Side-Loading
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5
  Risk Scores: Financial: 1.6, Safety: 1.6, Privacy: 8.0
  Risk Factors: exposure: 0.50, complexity: 0.70, attack_surface: 1.00
  Description: An adversary places a malicious version of a Dynamic-Link Library (DLL) in the Windows Side-by-Side (WinSxS) directory to trick the operating system into loading this malicious DLL instead of a legiti...

- Use of Captured Tickets (Pass The Ticket)
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5
  Risk Scores: Financial: 1.6, Safety: 1.6, Privacy: 8.0
  Risk Factors: exposure: 0.50, complexity: 0.70, attack_surface: 1.00
  Description: An adversary uses stolen Kerberos tickets to access systems/resources that leverage the Kerberos authentication protocol. The Kerberos authentication protocol centers around a ticketing system which i...

- Sniff Application Code
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5
  Risk Scores: Financial: 1.6, Safety: 1.6, Privacy: 8.0
  Risk Factors: exposure: 0.50, complexity: 0.70, attack_surface: 1.00
  Description: An adversary passively sniffs network communications and captures application code bound for an authorized client. Once obtained, they can use it as-is, or through reverse-engineering glean sensitive ...

- Exploitation of Transient Instruction Execution

Impact Scores: Financial: 1, Safety: 1, Privacy: 5
Risk Scores: Financial: 1.6, Safety: 1.6, Privacy: 8.0
Risk Factors: exposure: 0.50, complexity: 0.70, attack_surface: 1.00
Description: An adversary exploits a hardware design flaw in a CPU implementation of transient instruction execution to expose sensitive data and bypass/subvert access control over restricted resources. Typically,...

- Key Negotiation of Bluetooth Attack (KNOB)
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5
  Risk Scores: Financial: 1.6, Safety: 1.6, Privacy: 8.0
  Risk Factors: exposure: 0.50, complexity: 0.70, attack_surface: 1.00
  Description: An adversary can exploit a flaw in Bluetooth key negotiation allowing them to decrypt information sent between two devices communicating via Bluetooth. The adversary uses an Adversary in the Middle se...

- Software Development Tools Maliciously Altered
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5
  Risk Scores: Financial: 1.6, Safety: 1.6, Privacy: 8.0
  Risk Factors: exposure: 0.50, complexity: 0.70, attack_surface: 1.00
  Description: An adversary with the ability to alter tools used in a development environment causes software to be developed with maliciously modified tools. Such tools include requirements management and database ...

- Malicious Code Implanted During Chip Programming
  Impact Scores: Financial: 5, Safety: 1, Privacy: 1
  Risk Scores: Financial: 8.0, Safety: 1.6, Privacy: 1.6
  Risk Factors: exposure: 0.50, complexity: 0.70, attack_surface: 1.00
  Description: During the programming step of chip manufacture, an adversary with access and necessary technical skills maliciously alters a chip’s intended program logic to produce an effect intended by the adversa...

- Design for FPGA Maliciously Altered
  Impact Scores: Financial: 5, Safety: 1, Privacy: 1
  Risk Scores: Financial: 8.0, Safety: 1.6, Privacy: 1.6
  Risk Factors: exposure: 0.50, complexity: 0.70, attack_surface: 1.00
  Description: An adversary alters the functionality of a field-programmable gate array (FPGA) by causing an FPGA configuration memory chip reload in order to introduce a malicious function that could result in the ...

- System Build Data Maliciously Altered
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5
  Risk Scores: Financial: 1.6, Safety: 1.6, Privacy: 8.0
  Risk Factors: exposure: 0.50, complexity: 0.70, attack_surface: 1.00
  Description: During the system build process, the system is deliberately misconfigured by the alteration of the build data. Access to system configuration data files and build processes is susceptible to deliberat...

- Subvert Code-signing Facilities
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5
  Risk Scores: Financial: 1.6, Safety: 1.6, Privacy: 8.0
  Risk Factors: exposure: 0.50, complexity: 0.70, attack_surface: 1.00
  Description: Many languages use code signing facilities to vouch for code's identity and to thus tie code to its assigned privileges within an environment. Subverting this mechanism can be instrumental in an attac...

- Load Value Injection
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5
  Risk Scores: Financial: 1.6, Safety: 1.6, Privacy: 8.0
  Risk Factors: exposure: 0.50, complexity: 0.70, attack_surface: 1.00
  Description: An adversary exploits a hardware design flaw in a CPU implementation of transient instruction execution in

which a faulting or assisted load instruction transiently forwards adversary-controlled data ...

- DHCP Spoofing
  Impact Scores: Financial: 5, Safety: 1, Privacy: 1
  Risk Scores: Financial: 8.0, Safety: 1.6, Privacy: 1.6
  Risk Factors: exposure: 0.50, complexity: 0.70, attack_surface: 1.00
  Description: An adversary masquerades as a legitimate Dynamic Host Configuration Protocol (DHCP) server by spoofing DHCP traffic, with the goal of redirecting network traffic or denying service to DHCP....

- Active OS Fingerprinting
  Impact Scores: Financial: 1, Safety: 1, Privacy: 2.8
  Risk Scores: Financial: 2.4000000000000004, Safety: 2.4000000000000004, Privacy: 6.720000000000001
  Risk Factors: exposure: 0.50, complexity: 0.70, attack_surface: 1.00
  Description: An adversary engages in activity to detect the operating system or firmware version of a remote target by interrogating a device, server, or platform with a probe designed to solicit behavior that wil...

- TCP Timestamp Probe
  Impact Scores: Financial: 2.8, Safety: 1, Privacy: 1
  Risk Scores: Financial: 6.720000000000001, Safety: 2.4000000000000004, Privacy: 2.4000000000000004
  Risk Factors: exposure: 0.50, complexity: 0.70, attack_surface: 1.00
  Description: This OS fingerprinting probe examines the remote server's implementation of TCP timestamps. Not all operating systems implement timestamps within the TCP header, but when timestamps are used then this...

- TCP Sequence Number Probe
  Impact Scores: Financial: 2.8, Safety: 1, Privacy: 1
  Risk Scores: Financial: 6.720000000000001, Safety: 2.4000000000000004, Privacy: 2.4000000000000004
  Risk Factors: exposure: 0.50, complexity: 0.70, attack_surface: 1.00
  Description: This OS fingerprinting probe tests the target system's assignment of TCP sequence numbers. One common way to test TCP Sequence Number generation is to send a probe packet to an open port on the target...

- TCP (ISN) Greatest Common Divisor Probe
  Impact Scores: Financial: 1, Safety: 1, Privacy: 2.8
  Risk Scores: Financial: 2.4000000000000004, Safety: 2.4000000000000004, Privacy: 6.720000000000001
  Risk Factors: exposure: 0.50, complexity: 0.70, attack_surface: 1.00
  Description: This OS fingerprinting probe sends a number of TCP SYN packets to an open port of a remote machine. The Initial Sequence Number (ISN) in each of the SYN/ACK response packets is analyzed to determine t...

- TCP (ISN) Counter Rate Probe
  Impact Scores: Financial: 1, Safety: 1, Privacy: 2.8
  Risk Scores: Financial: 2.4000000000000004, Safety: 2.4000000000000004, Privacy: 6.720000000000001
  Risk Factors: exposure: 0.50, complexity: 0.70, attack_surface: 1.00
  Description: This OS detection probe measures the average rate of initial sequence number increments during a period of time. Sequence numbers are incremented using a time-based algorithm and are susceptible to a ...

- TCP (ISN) Sequence Predictability Probe
  Impact Scores: Financial: 1, Safety: 1, Privacy: 2.8
  Risk Scores: Financial: 2.4000000000000004, Safety: 2.4000000000000004, Privacy: 6.720000000000001
  Risk Factors: exposure: 0.50, complexity: 0.70, attack_surface: 1.00
  Description: This type of operating system probe attempts to determine an estimate for how predictable the sequence number generation algorithm is for a remote host. Statistical techniques, such as standard deviat...

- TCP Initial Window Size Probe
  Impact Scores: Financial: 2.8, Safety: 1, Privacy: 1

Risk Scores: Financial: 6.720000000000001, Safety: 2.4000000000000004, Privacy: 2.4000000000000004
Risk Factors: exposure: 0.50, complexity: 0.70, attack_surface: 1.00
Description: This OS fingerprinting probe checks the initial TCP Window size. TCP stacks limit the range of sequence numbers allowable within a session to maintain the connected state within TCP protocol logic. Th...

- TCP Options Probe
  Impact Scores: Financial: 2.8, Safety: 1, Privacy: 1
  Risk Scores: Financial: 6.720000000000001, Safety: 2.4000000000000004, Privacy: 2.4000000000000004
  Risk Factors: exposure: 0.50, complexity: 0.70, attack_surface: 1.00
  Description: This OS fingerprinting probe analyzes the type and order of any TCP header options present within a response segment. Most operating systems use unique ordering and different option sets when options ...

- Pretexting
  Impact Scores: Financial: 1, Safety: 1, Privacy: 2.8
  Risk Scores: Financial: 2.4000000000000004, Safety: 2.4000000000000004, Privacy: 6.720000000000001
  Risk Factors: exposure: 0.50, complexity: 0.70, attack_surface: 1.00
  Description: An adversary engages in pretexting behavior to solicit information from target persons, or manipulate the target into performing some action that serves the adversary's interests. During a pretexting ...

- Interception
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.199999999999999
  Risk Scores: Financial: 1.6, Safety: 1.6, Privacy: 6.719999999999999
  Risk Factors: exposure: 0.50, complexity: 0.70, attack_surface: 1.00
  Description: An adversary monitors data streams to or from the target for information gathering purposes. This attack may be undertaken to solely gather sensitive information or to support a further attack against...

- XML Ping of the Death
  Impact Scores: Financial: 1, Safety: 4.199999999999999, Privacy: 1
  Risk Scores: Financial: 1.6, Safety: 6.719999999999999, Privacy: 1.6
  Risk Factors: exposure: 0.50, complexity: 0.70, attack_surface: 1.00
  Description: An attacker initiates a resource depletion attack where a large number of small XML messages are delivered at a sufficiently rapid rate to cause a denial of service or crash of the target. Transaction...

- Incomplete Data Deletion in a Multi-Tenant Environment
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.199999999999999
  Risk Scores: Financial: 1.6, Safety: 1.6, Privacy: 6.719999999999999
  Risk Factors: exposure: 0.50, complexity: 0.70, attack_surface: 1.00
  Description: An adversary obtains unauthorized information due to insecure or incomplete data deletion in a multi-tenant environment. If a cloud provider fails to completely delete storage and data from former clo...

- Adding a Space to a File Extension
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.199999999999999
  Risk Scores: Financial: 1.6, Safety: 1.6, Privacy: 6.719999999999999
  Risk Factors: exposure: 0.50, complexity: 0.70, attack_surface: 1.00
  Description: An adversary adds a space character to the end of a file extension and takes advantage of an application that does not properly neutralize trailing special elements in file names. This extra space, wh...

- Reverse Engineering
  Impact Scores: Financial: 2.8, Safety: 1, Privacy: 1
  Risk Scores: Financial: 4.4799999999999995, Safety: 1.6, Privacy: 1.6
  Risk Factors: exposure: 0.50, complexity: 0.70, attack_surface: 1.00
  Description: An adversary discovers the structure, function, and composition of an object, resource, or system by using a variety of analysis techniques to effectively determine how the analyzed entity was constru...

- Fingerprinting
  Impact Scores: Financial: 1, Safety: 1, Privacy: 1.4
  Risk Scores: Financial: 3.2, Safety: 3.2, Privacy: 4.4799999999999995
  Risk Factors: exposure: 0.50, complexity: 0.70, attack_surface: 1.00
  Description: An adversary compares output from a target system to known indicators that uniquely identify specific details about the target. Most commonly, fingerprinting is done to determine operating system and ...

- Target Influence via Framing
  Impact Scores: Financial: 1, Safety: 1.4, Privacy: 2.8
  Risk Scores: Financial: 1.6, Safety: 2.2399999999999998, Privacy: 4.4799999999999995
  Risk Factors: exposure: 0.50, complexity: 0.70, attack_surface: 1.00
  Description: An adversary uses framing techniques to contextualize a conversation so that the target is more likely to be influenced by the adversary's point of view. Framing is information and experiences in life...

- Influence via Psychological Principles
  Impact Scores: Financial: 2.8, Safety: 1, Privacy: 1
  Risk Scores: Financial: 4.4799999999999995, Safety: 1.6, Privacy: 1.6
  Risk Factors: exposure: 0.50, complexity: 0.70, attack_surface: 1.00
  Description: The adversary shapes the target's actions or behavior by focusing on the ways human interact and learn, leveraging such elements as cognitive and social psychology. In a variety of ways, a target can ...

- File Discovery
  Impact Scores: Financial: 1.4, Safety: 1, Privacy: 1
  Risk Scores: Financial: 4.4799999999999995, Safety: 3.2, Privacy: 3.2
  Risk Factors: exposure: 0.50, complexity: 0.70, attack_surface: 1.00
  Description: An adversary engages in probing and exploration activities to determine if common key files exists. Such files often contain configuration and security parameters of the targeted application, system o...

- Process Footprinting
  Impact Scores: Financial: 1, Safety: 1, Privacy: 2.8
  Risk Scores: Financial: 1.6, Safety: 1.6, Privacy: 4.4799999999999995
  Risk Factors: exposure: 0.50, complexity: 0.70, attack_surface: 1.00
  Description: An adversary exploits functionality meant to identify information about the currently running processes on the target system to an authorized user. By knowing what processes are running on the target ...

- Services Footprinting
  Impact Scores: Financial: 1, Safety: 1, Privacy: 2.8
  Risk Scores: Financial: 1.6, Safety: 1.6, Privacy: 4.4799999999999995
  Risk Factors: exposure: 0.50, complexity: 0.70, attack_surface: 1.00
  Description: An adversary exploits functionality meant to identify information about the services on the target system to an authorized user. By knowing what services are registered on the target system, the adver...

- Account Footprinting
  Impact Scores: Financial: 1, Safety: 1, Privacy: 2.8
  Risk Scores: Financial: 1.6, Safety: 1.6, Privacy: 4.4799999999999995
  Risk Factors: exposure: 0.50, complexity: 0.70, attack_surface: 1.00
  Description: An adversary exploits functionality meant to identify information about the domain accounts and their permissions on the target system to an authorized user. By knowing what accounts are registered on...

- Group Permission Footprinting
  Impact Scores: Financial: 1, Safety: 1, Privacy: 2.8
  Risk Scores: Financial: 1.6, Safety: 1.6, Privacy: 4.4799999999999995
  Risk Factors: exposure: 0.50, complexity: 0.70, attack_surface: 1.00

Description: An adversary exploits functionality meant to identify information about user groups and their permissions on the target system to an authorized user. By knowing what users/permissions are registered o...

- Owner Footprinting
  Impact Scores: Financial: 1, Safety: 1, Privacy: 2.8
  Risk Scores: Financial: 1.6, Safety: 1.6, Privacy: 4.4799999999999995
  Risk Factors: exposure: 0.50, complexity: 0.70, attack_surface: 1.00
  Description: An adversary exploits functionality meant to identify information about the primary users on the target system to an authorized user. They may do this, for example, by reviewing logins or file modific...

- System Footprinting
  Impact Scores: Financial: 1, Safety: 1, Privacy: 2.8
  Risk Scores: Financial: 1.6, Safety: 1.6, Privacy: 4.4799999999999995
  Risk Factors: exposure: 0.50, complexity: 0.70, attack_surface: 1.00
  Description: An adversary engages in active probing and exploration activities to determine security information about a remote target system. Often times adversaries will rely on remote applications that can be p...

- Collect Data from Clipboard
  Impact Scores: Financial: 1, Safety: 1, Privacy: 2.8
  Risk Scores: Financial: 1.6, Safety: 1.6, Privacy: 4.4799999999999995
  Risk Factors: exposure: 0.50, complexity: 0.70, attack_surface: 1.00
  Description: The adversary exploits an application that allows for the copying of sensitive data or information by collecting information copied to the clipboard. Data copied to the clipboard can be accessed by ot...

Component: Transmission Control Unit

Type: ECU
Safety Level: ASIL C
Interfaces: CAN, FlexRay
Access Points: Debug Port
Data Types: Sensor Data, Control Commands
Location: Internal
Trust Zone: Critical
Connected To: ECU003, ECU001

Identified Threats:

- Buffer Manipulation
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5
  Risk Scores: Financial: 2.84, Safety: 2.84, Privacy: 14.2
  Risk Factors: exposure: 0.50, complexity: 0.60, attack_surface: 0.70
  Description: An adversary manipulates an application's interaction with a buffer in an attempt to read or modify data they shouldn't have access to. Buffer attacks are distinguished in that it is the buffer space ...

- Redirect Access to Libraries
  Impact Scores: Financial: 1, Safety: 5, Privacy: 1
  Risk Scores: Financial: 2.84, Safety: 14.2, Privacy: 2.84
  Risk Factors: exposure: 0.50, complexity: 0.60, attack_surface: 0.70
  Description: An adversary exploits a weakness in the way an application searches for external libraries to manipulate the execution flow to point to an adversary supplied library or code base. This pattern of atta...

- XSS Targeting Non-Script Elements
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5
  Risk Scores: Financial: 2.84, Safety: 2.84, Privacy: 14.2
  Risk Factors: exposure: 0.50, complexity: 0.60, attack_surface: 0.70
  Description: This attack is a form of Cross-Site Scripting (XSS) where malicious scripts are embedded in elements that are not expected to host scripts such as image tags (<img>), comments in XML documents (< !-CD...

- Leverage Executable Code in Non-Executable Files
  Impact Scores: Financial: 5, Safety: 1, Privacy: 1
  Risk Scores: Financial: 14.2, Safety: 2.84, Privacy: 2.84
  Risk Factors: exposure: 0.50, complexity: 0.60, attack_surface: 0.70
  Description: An attack of this type exploits a system's trust in configuration and resource files. When the executable loads the resource (such as an image file or configuration file) the attacker has modified the...

- Retrieve Embedded Sensitive Data
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5
  Risk Scores: Financial: 2.84, Safety: 2.84, Privacy: 14.2
  Risk Factors: exposure: 0.50, complexity: 0.60, attack_surface: 0.70
  Description: An attacker examines a target system to find sensitive data that has been embedded within it. This information can reveal confidential contents, such as account numbers or individual keys/credentials ...

- Leveraging/Manipulating Configuration File Search Paths
  Impact Scores: Financial: 5, Safety: 1, Privacy: 1
  Risk Scores: Financial: 14.2, Safety: 2.84, Privacy: 2.84
  Risk Factors: exposure: 0.50, complexity: 0.60, attack_surface: 0.70
  Description: This pattern of attack sees an adversary load a malicious resource into a program's standard path so that when a known command is executed then the system instead executes the malicious component. The...

- Manipulating Writeable Terminal Devices
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5
  Risk Scores: Financial: 2.84, Safety: 2.84, Privacy: 14.2
  Risk Factors: exposure: 0.50, complexity: 0.60, attack_surface: 0.70
  Description: This attack exploits terminal devices that allow themselves to be written to by other users. The attacker sends command strings to the target terminal device hoping that the target user will hit enter...

- Overflow Binary Resource File
  Impact Scores: Financial: 5, Safety: 1, Privacy: 1
  Risk Scores: Financial: 14.2, Safety: 2.84, Privacy: 2.84
  Risk Factors: exposure: 0.50, complexity: 0.60, attack_surface: 0.70
  Description: An attack of this type exploits a buffer overflow vulnerability in the handling of binary resources. Binary resources may include music files like MP3, image files like JPEG files, and any other binar...

- Poison Web Service Registry
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5
  Risk Scores: Financial: 2.84, Safety: 2.84, Privacy: 14.2
  Risk Factors: exposure: 0.50, complexity: 0.60, attack_surface: 0.70
  Description: SOA and Web Services often use a registry to perform look up, get schema information, and metadata about services. A poisoned registry can redirect (think phishing for servers) the service requester t...

- String Format Overflow in syslog()
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5
  Risk Scores: Financial: 2.84, Safety: 2.84, Privacy: 14.2
  Risk Factors: exposure: 0.50, complexity: 0.60, attack_surface: 0.70

Description: This attack targets applications and software that uses the syslog() function insecurely. If an application does not explicitely use a format string parameter in a call to syslog(), user input can be ...

- Manipulating User-Controlled Variables
  Impact Scores: Financial: 2.4, Safety: 1, Privacy: 5
  Risk Scores: Financial: 6.816, Safety: 2.84, Privacy: 14.2
  Risk Factors: exposure: 0.50, complexity: 0.60, attack_surface: 0.70
  Description: This attack targets user controlled variables (DEBUG=1, PHP Globals, and So Forth). An adversary can override variables leveraging user-supplied, untrusted query variables directly used on the applica...

- XQuery Injection
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5
  Risk Scores: Financial: 2.84, Safety: 2.84, Privacy: 14.2
  Risk Factors: exposure: 0.50, complexity: 0.60, attack_surface: 0.70
  Description: This attack utilizes XQuery to probe and attack server systems; in a similar manner that SQL Injection allows an attacker to exploit SQL calls to RDBMS, XQuery Injection uses improperly validated data...

- Pharming
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5
  Risk Scores: Financial: 2.84, Safety: 2.84, Privacy: 14.2
  Risk Factors: exposure: 0.50, complexity: 0.60, attack_surface: 0.70
  Description: A pharming attack occurs when the victim is fooled into entering sensitive data into supposedly trusted locations, such as an online bank site or a trading platform. An attacker can impersonate these ...

- Phishing
  Impact Scores: Financial: 1.2, Safety: 1, Privacy: 5
  Risk Scores: Financial: 3.408, Safety: 2.84, Privacy: 14.2
  Risk Factors: exposure: 0.50, complexity: 0.60, attack_surface: 0.70
  Description: Phishing is a social engineering technique where an attacker masquerades as a legitimate entity with which the victim might do business in order to prompt the user to reveal some confidential informat...

- Accessing Functionality Not Properly Constrained by ACLs
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.8
  Risk Scores: Financial: 2.84, Safety: 2.84, Privacy: 13.632
  Risk Factors: exposure: 0.50, complexity: 0.60, attack_surface: 0.70
  Description: In applications, particularly web applications, access to functionality is mitigated by an authorization framework. This framework maps Access Control Lists (ACLs) to elements of the application's fun...

- Buffer Overflow via Environment Variables
  Impact Scores: Financial: 4.8, Safety: 1, Privacy: 1
  Risk Scores: Financial: 13.632, Safety: 2.84, Privacy: 2.84
  Risk Factors: exposure: 0.50, complexity: 0.60, attack_surface: 0.70
  Description: This attack pattern involves causing a buffer overflow through manipulation of environment variables. Once the adversary finds that they can modify an environment variable, they may try to overflow as...

- Server Side Include (SSI) Injection
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.8
  Risk Scores: Financial: 2.84, Safety: 2.84, Privacy: 13.632
  Risk Factors: exposure: 0.50, complexity: 0.60, attack_surface: 0.70
  Description: An attacker can use Server Side Include (SSI) Injection to send code to a web application that then gets executed by the web server. Doing so enables the attacker to achieve similar results to Cross S...

- Format String Injection

Impact Scores: Financial: 1, Safety: 2.4, Privacy: 4.8
Risk Scores: Financial: 2.84, Safety: 6.816, Privacy: 13.632
Risk Factors: exposure: 0.50, complexity: 0.60, attack_surface: 0.70
Description: An adversary includes formatting characters in a string input field on the target application. Most applications assume that users will provide static text and may respond unpredictably to the presenc...

- Cache Poisoning
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.8
  Risk Scores: Financial: 2.84, Safety: 2.84, Privacy: 13.632
  Risk Factors: exposure: 0.50, complexity: 0.60, attack_surface: 0.70
  Description: An attacker exploits the functionality of cache technologies to cause specific data to be cached that aids the attackers' objectives. This describes any attack whereby an attacker places incorrect or ...

- DNS Cache Poisoning
  Impact Scores: Financial: 4.8, Safety: 1, Privacy: 1
  Risk Scores: Financial: 13.632, Safety: 2.84, Privacy: 2.84
  Risk Factors: exposure: 0.50, complexity: 0.60, attack_surface: 0.70
  Description: A domain name server translates a domain name (such as www.example.com) into an IP address that Internet hosts use to contact Internet resources. An adversary modifies a public DNS cache to cause cert...

- Command Delimiters
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.8
  Risk Scores: Financial: 2.84, Safety: 2.84, Privacy: 13.632
  Risk Factors: exposure: 0.50, complexity: 0.60, attack_surface: 0.70
  Description: An attack of this type exploits a programs' vulnerabilities that allows an attacker's commands to be concatenated onto a legitimate command with the intent of targeting other resources such as the fil...

- Malicious Automated Software Update via Redirection
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.8
  Risk Scores: Financial: 2.84, Safety: 2.84, Privacy: 13.632
  Risk Factors: exposure: 0.50, complexity: 0.60, attack_surface: 0.70
  Description: An attacker exploits two layers of weaknesses in server or client software for automated update mechanisms to undermine the integrity of the target code-base. The first weakness involves a failure to ...

- PHP Remote File Inclusion
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.8
  Risk Scores: Financial: 2.84, Safety: 2.84, Privacy: 13.632
  Risk Factors: exposure: 0.50, complexity: 0.60, attack_surface: 0.70
  Description: In this pattern the adversary is able to load and execute arbitrary code remotely available from the application. This is usually accomplished through an insecurely configured PHP runtime environment ...

- XSS Using Alternate Syntax
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.8
  Risk Scores: Financial: 2.84, Safety: 2.84, Privacy: 13.632
  Risk Factors: exposure: 0.50, complexity: 0.60, attack_surface: 0.70
  Description: An adversary uses alternate forms of keywords or commands that result in the same action as the primary form but which may not be caught by filters. For example, many keywords are processed in a case ...

- Serialized Data External Linking
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.8
  Risk Scores: Financial: 2.84, Safety: 2.84, Privacy: 13.632
  Risk Factors: exposure: 0.50, complexity: 0.60, attack_surface: 0.70
  Description: An adversary creates a serialized data file (e.g. XML, YAML, etc...) that contains an external data

reference. Because serialized data parsers may not validate documents with external references, ther...

- Leveraging Race Conditions
  Impact Scores: Financial: 4.8, Safety: 1, Privacy: 1
  Risk Scores: Financial: 13.632, Safety: 2.84, Privacy: 2.84
  Risk Factors: exposure: 0.50, complexity: 0.60, attack_surface: 0.70
  Description: The adversary targets a race condition occurring when multiple processes access and manipulate the same resource concurrently, and the outcome of the execution depends on the particular order in which...

- Leveraging Time-of-Check and Time-of-Use (TOCTOU) Race Conditions
  Impact Scores: Financial: 4.8, Safety: 1, Privacy: 1
  Risk Scores: Financial: 13.632, Safety: 2.84, Privacy: 2.84
  Risk Factors: exposure: 0.50, complexity: 0.60, attack_surface: 0.70
  Description: This attack targets a race condition occurring between the time of check (state) for a resource and the time of use of a resource. A typical example is file access. The adversary can leverage a file a...

- Using Meta-characters in E-mail Headers to Inject Malicious Payloads
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.8
  Risk Scores: Financial: 2.84, Safety: 2.84, Privacy: 13.632
  Risk Factors: exposure: 0.50, complexity: 0.60, attack_surface: 0.70
  Description: This type of attack involves an attacker leveraging meta-characters in email headers to inject improper behavior into email programs. Email software has become increasingly sophisticated and feature-r...

- Buffer Overflow via Symbolic Links
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.8
  Risk Scores: Financial: 2.84, Safety: 2.84, Privacy: 13.632
  Risk Factors: exposure: 0.50, complexity: 0.60, attack_surface: 0.70
  Description: This type of attack leverages the use of symbolic links to cause buffer overflows. An adversary can try to create or manipulate a symbolic link file such that its contents result in out of bounds data...

- Passing Local Filenames to Functions That Expect a URL
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.8
  Risk Scores: Financial: 2.84, Safety: 2.84, Privacy: 13.632
  Risk Factors: exposure: 0.50, complexity: 0.60, attack_surface: 0.70
  Description: This attack relies on client side code to access local files and resources instead of URLs. When the client browser is expecting a URL string, but instead receives a request for a local file, that exe...

- Session Credential Falsification through Prediction
  Impact Scores: Financial: 4.8, Safety: 1, Privacy: 1
  Risk Scores: Financial: 13.632, Safety: 2.84, Privacy: 2.84
  Risk Factors: exposure: 0.50, complexity: 0.60, attack_surface: 0.70
  Description: This attack targets predictable session ID in order to gain privileges. The attacker can predict the session ID used during a transaction to perform spoofing and session hijacking....

- Using Slashes and URL Encoding Combined to Bypass Validation Logic
  Impact Scores: Financial: 4.8, Safety: 1, Privacy: 1
  Risk Scores: Financial: 13.632, Safety: 2.84, Privacy: 2.84
  Risk Factors: exposure: 0.50, complexity: 0.60, attack_surface: 0.70
  Description: This attack targets the encoding of the URL combined with the encoding of the slash characters. An attacker can take advantage of the multiple ways of encoding a URL and abuse the interpretation of th...

- Avoid Security Tool Identification by Adding Data
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.8

Risk Scores: Financial: 2.84, Safety: 2.84, Privacy: 13.632
Risk Factors: exposure: 0.50, complexity: 0.60, attack_surface: 0.70
Description: An adversary adds data to a file to increase the file size beyond what security tools are capable of handling in an attempt to mask their actions. In addition to this, adding data to a file also chang...

- Voice Phishing
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.8
  Risk Scores: Financial: 2.84, Safety: 2.84, Privacy: 13.632
  Risk Factors: exposure: 0.50, complexity: 0.60, attack_surface: 0.70
  Description: An adversary targets users with a phishing attack for the purpose of soliciting account passwords or sensitive information from the user. Voice Phishing is a variation of the Phishing social engineeri...

- Malicious Automated Software Update via Spoofing
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.8
  Risk Scores: Financial: 2.84, Safety: 2.84, Privacy: 13.632
  Risk Factors: exposure: 0.50, complexity: 0.60, attack_surface: 0.70
  Description: An attackers uses identify or content spoofing to trick a client into performing an automated software update from a malicious source. A malicious automated software update that leverages spoofing can...

- Blind SQL Injection
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.8
  Risk Scores: Financial: 2.84, Safety: 2.84, Privacy: 13.632
  Risk Factors: exposure: 0.50, complexity: 0.60, attack_surface: 0.70
  Description: Blind SQL Injection results from an insufficient mitigation for SQL Injection. Although suppressing database error messages are considered best practice, the suppression alone is not sufficient to pre...

- URL Encoding
  Impact Scores: Financial: 4.8, Safety: 1, Privacy: 1
  Risk Scores: Financial: 13.632, Safety: 2.84, Privacy: 2.84
  Risk Factors: exposure: 0.50, complexity: 0.60, attack_surface: 0.70
  Description: This attack targets the encoding of the URL. An adversary can take advantage of the multiple way of encoding an URL and abuse the interpretation of the URL....

- User-Controlled Filename
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.8
  Risk Scores: Financial: 2.84, Safety: 2.84, Privacy: 13.632
  Risk Factors: exposure: 0.50, complexity: 0.60, attack_surface: 0.70
  Description: An attack of this type involves an adversary inserting malicious characters (such as a XSS redirection) into a filename, directly or indirectly that is then used by the target software to generate HTM...

- Using Escaped Slashes in Alternate Encoding
  Impact Scores: Financial: 4.8, Safety: 1, Privacy: 1
  Risk Scores: Financial: 13.632, Safety: 2.84, Privacy: 2.84
  Risk Factors: exposure: 0.50, complexity: 0.60, attack_surface: 0.70
  Description: This attack targets the use of the backslash in alternate encoding. An adversary can provide a backslash as a leading character and causes a parser to believe that the next character is special. This ...

- Buffer Overflow in an API Call
  Impact Scores: Financial: 4.8, Safety: 1, Privacy: 1
  Risk Scores: Financial: 13.632, Safety: 2.84, Privacy: 2.84
  Risk Factors: exposure: 0.50, complexity: 0.60, attack_surface: 0.70
  Description: This attack targets libraries or shared code modules which are vulnerable to buffer overflow attacks. An adversary who has knowledge of known vulnerable libraries or shared code can easily target soft...

- Using UTF-8 Encoding to Bypass Validation Logic
  Impact Scores: Financial: 1, Safety: 4.8, Privacy: 1
  Risk Scores: Financial: 2.84, Safety: 13.632, Privacy: 2.84
  Risk Factors: exposure: 0.50, complexity: 0.60, attack_surface: 0.70
  Description: This attack is a specific variation on leveraging alternate encodings to bypass validation logic. This attack leverages the possibility to encode potentially harmful input in UTF-8 and submit it to ap...

- XPath Injection
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.8
  Risk Scores: Financial: 2.84, Safety: 2.84, Privacy: 13.632
  Risk Factors: exposure: 0.50, complexity: 0.60, attack_surface: 0.70
  Description: An attacker can craft special user-controllable input consisting of XPath expressions to inject the XML database and bypass authentication or glean information that they normally would not be able to....

- OS Command Injection
  Impact Scores: Financial: 4.8, Safety: 1, Privacy: 1
  Risk Scores: Financial: 13.632, Safety: 2.84, Privacy: 2.84
  Risk Factors: exposure: 0.50, complexity: 0.60, attack_surface: 0.70
  Description: In this type of an attack, an adversary injects operating system commands into existing application functions. An application that uses untrusted input to build command strings is vulnerable. An adver...

- Buffer Overflow in Local Command-Line Utilities
  Impact Scores: Financial: 4.8, Safety: 1, Privacy: 1
  Risk Scores: Financial: 13.632, Safety: 2.84, Privacy: 2.84
  Risk Factors: exposure: 0.50, complexity: 0.60, attack_surface: 0.70
  Description: This attack targets command-line utilities available in a number of shells. An adversary can leverage a vulnerability found in a command-line utility to escalate privilege to root....

- Reflection Attack in Authentication Protocol
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.8
  Risk Scores: Financial: 2.84, Safety: 2.84, Privacy: 13.632
  Risk Factors: exposure: 0.50, complexity: 0.60, attack_surface: 0.70
  Description: An adversary can abuse an authentication protocol susceptible to reflection attack in order to defeat it. Doing so allows the adversary illegitimate access to the target system, without possessing the...

- Forced Integer Overflow
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.8
  Risk Scores: Financial: 2.84, Safety: 2.84, Privacy: 13.632
  Risk Factors: exposure: 0.50, complexity: 0.60, attack_surface: 0.70
  Description: This attack forces an integer variable to go out of range. The integer variable is often used as an offset such as size of memory allocation or similarly. The attacker would typically control the valu...

- WSDL Scanning
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.8
  Risk Scores: Financial: 2.84, Safety: 2.84, Privacy: 13.632
  Risk Factors: exposure: 0.50, complexity: 0.60, attack_surface: 0.70
  Description: This attack targets the WSDL interface made available by a web service. The attacker may scan the WSDL interface to reveal sensitive information about invocation patterns, underlying technology implem...

- Root/Jailbreak Detection Evasion via Debugging
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5
  Risk Scores: Financial: 2.13, Safety: 2.13, Privacy: 10.649999999999999
  Risk Factors: exposure: 0.50, complexity: 0.60, attack_surface: 0.70

Description: An adversary inserts a debugger into the program entry point of a mobile application to modify the application binary, with the goal of evading Root/Jailbreak detection. Mobile device users often Root...

- Exploitation of Improperly Controlled Hardware Security Identifiers
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5
  Risk Scores: Financial: 2.13, Safety: 2.13, Privacy: 10.649999999999999
  Risk Factors: exposure: 0.50, complexity: 0.60, attack_surface: 0.70
  Description: An adversary takes advantage of missing or incorrectly configured security identifiers (e.g., tokens), which are used for access control within a System-on-Chip (SoC), to read/write data or execute a ...

- CAN Injection
  Impact Scores: Financial: 3.5999999999999996, Safety: 4.8, Privacy: 2.4
  Risk Scores: Financial: 7.667999999999999, Safety: 10.223999999999998, Privacy: 5.111999999999999
  Risk Factors: exposure: 0.50, complexity: 0.60, attack_surface: 0.70
  Description: Manipulation of CAN bus messages leading to vehicle malfunction...

- Sensor Data Manipulation
  Impact Scores: Financial: 3.5999999999999996, Safety: 4.8, Privacy: 2.4
  Risk Scores: Financial: 7.667999999999999, Safety: 10.223999999999998, Privacy: 5.111999999999999
  Risk Factors: exposure: 0.50, complexity: 0.60, attack_surface: 0.70
  Description: Tampering with sensor data leading to incorrect vehicle behavior...

- HTTP Request Splitting
  Impact Scores: Financial: 4.8, Safety: 1, Privacy: 1
  Risk Scores: Financial: 10.223999999999998, Safety: 2.13, Privacy: 2.13
  Risk Factors: exposure: 0.50, complexity: 0.60, attack_surface: 0.70
  Description: An adversary abuses the flexibility and discrepancies in the parsing and interpretation of HTTP Request messages by different intermediary HTTP agents (e.g., load balancer, reverse proxy, web caching ...

- Flooding
  Impact Scores: Financial: 1, Safety: 1.2, Privacy: 3.5999999999999996
  Risk Scores: Financial: 2.84, Safety: 3.408, Privacy: 10.223999999999998
  Risk Factors: exposure: 0.50, complexity: 0.60, attack_surface: 0.70
  Description: An adversary consumes the resources of a target by rapidly engaging in a large number of interactions with the target. This type of attack generally exposes a weakness in rate limiting or flow. When s...

- Directory Indexing
  Impact Scores: Financial: 1, Safety: 1, Privacy: 3.5999999999999996
  Risk Scores: Financial: 2.84, Safety: 2.84, Privacy: 10.223999999999998
  Risk Factors: exposure: 0.50, complexity: 0.60, attack_surface: 0.70
  Description: An adversary crafts a request to a target that results in the target listing/indexing the content of a directory as output. One common method of triggering directory contents as output is to construct...

- Flash Parameter Injection
  Impact Scores: Financial: 1, Safety: 1, Privacy: 3.5999999999999996
  Risk Scores: Financial: 2.84, Safety: 2.84, Privacy: 10.223999999999998
  Risk Factors: exposure: 0.50, complexity: 0.60, attack_surface: 0.70
  Description: An adversary takes advantage of improper data validation to inject malicious global parameters into a Flash file embedded within an HTML document. Flash files can leverage user-submitted data to confi...

- Exploiting Incorrectly Configured Access Control Security Levels
  Impact Scores: Financial: 1, Safety: 1, Privacy: 3.5999999999999996
  Risk Scores: Financial: 2.84, Safety: 2.84, Privacy: 10.223999999999998

Risk Factors: exposure: 0.50, complexity: 0.60, attack_surface: 0.70
Description: An attacker exploits a weakness in the configuration of access controls and is able to bypass the intended protection that these measures guard against and thereby obtain unauthorized access to the sy...

- Exponential Data Expansion
  Impact Scores: Financial: 1, Safety: 1, Privacy: 3.5999999999999996
  Risk Scores: Financial: 2.84, Safety: 2.84, Privacy: 10.223999999999998
  Risk Factors: exposure: 0.50, complexity: 0.60, attack_surface: 0.70
  Description: An adversary submits data to a target application which contains nested exponential data expansion to produce excessively large output. Many data format languages allow the definition of macro-like st...

- Inducing Account Lockout
  Impact Scores: Financial: 1, Safety: 1, Privacy: 3.5999999999999996
  Risk Scores: Financial: 2.84, Safety: 2.84, Privacy: 10.223999999999998
  Risk Factors: exposure: 0.50, complexity: 0.60, attack_surface: 0.70
  Description: An attacker leverages the security functionality of the system aimed at thwarting potential attacks to launch a denial of service attack against a legitimate system user. Many systems, for instance, i...

- XML Routing Detour Attacks
  Impact Scores: Financial: 1, Safety: 1, Privacy: 3.5999999999999996
  Risk Scores: Financial: 2.84, Safety: 2.84, Privacy: 10.223999999999998
  Risk Factors: exposure: 0.50, complexity: 0.60, attack_surface: 0.70
  Description: An attacker subverts an intermediate system used to process XML content and forces the intermediate to modify and/or re-route the processing of the content. XML Routing Detour Attacks are Adversary in...

- Serialized Data with Nested Payloads
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.8
  Risk Scores: Financial: 2.13, Safety: 2.13, Privacy: 10.223999999999998
  Risk Factors: exposure: 0.50, complexity: 0.60, attack_surface: 0.70
  Description: Applications often need to transform data in and out of a data format (e.g., XML and YAML) by using a parser. It may be possible for an adversary to inject data that may have an adverse effect on the ...

- Command Injection
  Impact Scores: Financial: 4.8, Safety: 1, Privacy: 1
  Risk Scores: Financial: 10.223999999999998, Safety: 2.13, Privacy: 2.13
  Risk Factors: exposure: 0.50, complexity: 0.60, attack_surface: 0.70
  Description: An adversary looking to execute a command of their choosing, injects new items into an existing command thus modifying interpretation away from what was intended. Commands in this context are often st...

- Leveraging Race Conditions via Symbolic Links
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.8
  Risk Scores: Financial: 2.13, Safety: 2.13, Privacy: 10.223999999999998
  Risk Factors: exposure: 0.50, complexity: 0.60, attack_surface: 0.70
  Description: This attack leverages the use of symbolic links (Symlinks) in order to write to sensitive files. An attacker can create a Symlink link to a target file not otherwise accessible to them. When the privi...

- HTTP Response Smuggling
  Impact Scores: Financial: 4.8, Safety: 1, Privacy: 1
  Risk Scores: Financial: 10.223999999999998, Safety: 2.13, Privacy: 2.13
  Risk Factors: exposure: 0.50, complexity: 0.60, attack_surface: 0.70
  Description: An adversary manipulates and injects malicious content in the form of secret unauthorized HTTP responses, into a single HTTP response from a vulnerable or compromised back-end HTTP agent (e.g., server...

- SOAP Manipulation
  Impact Scores: Financial: 4.8, Safety: 1, Privacy: 1
  Risk Scores: Financial: 10.223999999999998, Safety: 2.13, Privacy: 2.13
  Risk Factors: exposure: 0.50, complexity: 0.60, attack_surface: 0.70
  Description: Simple Object Access Protocol (SOAP) is used as a communication protocol between a client and server to invoke web services on the server. It is an XML-based protocol, and therefore suffers from many ...

- Fuzzing
  Impact Scores: Financial: 1, Safety: 1, Privacy: 3.5999999999999996
  Risk Scores: Financial: 2.84, Safety: 2.84, Privacy: 10.223999999999998
  Risk Factors: exposure: 0.50, complexity: 0.60, attack_surface: 0.70
  Description: In this attack pattern, the adversary leverages fuzzing to try to identify weaknesses in the system. Fuzzing is a software security and functionality testing method that feeds randomly constructed inp...

- HTTP Request Smuggling
  Impact Scores: Financial: 4.8, Safety: 1, Privacy: 1
  Risk Scores: Financial: 10.223999999999998, Safety: 2.13, Privacy: 2.13
  Risk Factors: exposure: 0.50, complexity: 0.60, attack_surface: 0.70
  Description: An adversary abuses the flexibility and discrepancies in the parsing and interpretation of HTTP Request messages using various HTTP headers, request-line and body parameters as well as message sizes (...

- HTTP Response Splitting
  Impact Scores: Financial: 4.8, Safety: 1, Privacy: 1
  Risk Scores: Financial: 10.223999999999998, Safety: 2.13, Privacy: 2.13
  Risk Factors: exposure: 0.50, complexity: 0.60, attack_surface: 0.70
  Description: An adversary manipulates and injects malicious content, in the form of secret unauthorized HTTP responses, into a single HTTP response from a vulnerable or compromised back-end HTTP agent (e.g., web s...

- Manipulating Opaque Client-based Data Tokens
  Impact Scores: Financial: 1, Safety: 1, Privacy: 3.5999999999999996
  Risk Scores: Financial: 2.84, Safety: 2.84, Privacy: 10.223999999999998
  Risk Factors: exposure: 0.50, complexity: 0.60, attack_surface: 0.70
  Description: In circumstances where an application holds important data client-side in tokens (cookies, URLs, data files, and so forth) that data can be manipulated. If client or server-side application components...

- Using Alternative IP Address Encodings
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.8
  Risk Scores: Financial: 2.13, Safety: 2.13, Privacy: 10.223999999999998
  Risk Factors: exposure: 0.50, complexity: 0.60, attack_surface: 0.70
  Description: This attack relies on the adversary using unexpected formats for representing IP addresses. Networked applications may expect network location information in a specific format, such as fully qualified...

- Exploiting Multiple Input Interpretation Layers
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.8
  Risk Scores: Financial: 2.13, Safety: 2.13, Privacy: 10.223999999999998
  Risk Factors: exposure: 0.50, complexity: 0.60, attack_surface: 0.70
  Description: An attacker supplies the target software with input data that contains sequences of special characters designed to bypass input validation logic. This exploit relies on the target making multiples pas...

- Development Alteration
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.8
  Risk Scores: Financial: 2.13, Safety: 2.13, Privacy: 10.223999999999998
  Risk Factors: exposure: 0.50, complexity: 0.60, attack_surface: 0.70

Description: An adversary modifies a technology, product, or component during its development to acheive a negative impact once the system is deployed. The goal of the adversary is to modify the system in such a w...

- Malicious Logic Insertion into Product Software via Configuration Management Manipulation
  Impact Scores: Financial: 4.8, Safety: 1, Privacy: 1
  Risk Scores: Financial: 10.223999999999998, Safety: 2.13, Privacy: 2.13
  Risk Factors: exposure: 0.50, complexity: 0.60, attack_surface: 0.70
  Description: An adversary exploits a configuration management system so that malicious logic is inserted into a software products build, update or deployed environment. If an adversary can control the elements inc...

- Design Alteration
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.8
  Risk Scores: Financial: 2.13, Safety: 2.13, Privacy: 10.223999999999998
  Risk Factors: exposure: 0.50, complexity: 0.60, attack_surface: 0.70
  Description: An adversary modifies the design of a technology, product, or component to acheive a negative impact once the system is deployed. In this type of attack, the goal of the adversary is to modify the des...

- Contradictory Destinations in Traffic Routing Schemes
  Impact Scores: Financial: 4.8, Safety: 1, Privacy: 1
  Risk Scores: Financial: 10.223999999999998, Safety: 2.13, Privacy: 2.13
  Risk Factors: exposure: 0.50, complexity: 0.60, attack_surface: 0.70
  Description: Adversaries can provide contradictory destinations when sending messages. Traffic is routed in networks using the domain names in various headers available at different levels of the OSI model. In a C...

- Local Execution of Code
  Impact Scores: Financial: 4.8, Safety: 1, Privacy: 1
  Risk Scores: Financial: 10.223999999999998, Safety: 2.13, Privacy: 2.13
  Risk Factors: exposure: 0.50, complexity: 0.60, attack_surface: 0.70
  Description: An adversary installs and executes malicious code on the target system in an effort to achieve a negative technical impact. Examples include rootkits, ransomware, spyware, adware, and others....

- Object Injection
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.8
  Risk Scores: Financial: 2.13, Safety: 2.13, Privacy: 10.223999999999998
  Risk Factors: exposure: 0.50, complexity: 0.60, attack_surface: 0.70
  Description: An adversary attempts to exploit an application by injecting additional, malicious content during its processing of serialized objects. Developers leverage serialization in order to convert data or st...

- Bluetooth Impersonation AttackS (BIAS)
  Impact Scores: Financial: 4.8, Safety: 1, Privacy: 1
  Risk Scores: Financial: 10.223999999999998, Safety: 2.13, Privacy: 2.13
  Risk Factors: exposure: 0.50, complexity: 0.60, attack_surface: 0.70
  Description: An adversary disguises the MAC address of their Bluetooth enabled device to one for which there exists an active and trusted connection and authenticates successfully. The adversary can then perform m...

- Alteration of a Software Update
  Impact Scores: Financial: 4.8, Safety: 1, Privacy: 1
  Risk Scores: Financial: 10.223999999999998, Safety: 2.13, Privacy: 2.13
  Risk Factors: exposure: 0.50, complexity: 0.60, attack_surface: 0.70
  Description: An adversary with access to an organization’s software update infrastructure inserts malware into the content of an outgoing update to fielded systems where a wide range of malicious effects are possi...

- Eavesdropping on a Monitor

Impact Scores: Financial: 1, Safety: 1, Privacy: 4.8
Risk Scores: Financial: 2.13, Safety: 2.13, Privacy: 10.223999999999998
Risk Factors: exposure: 0.50, complexity: 0.60, attack_surface: 0.70
Description: An Adversary can eavesdrop on the content of an external monitor through the air without modifying any cable or installing software, just capturing this signal emitted by the cable or video port, with...

- Browser in the Middle (BiTM)
  Impact Scores: Financial: 4.8, Safety: 1, Privacy: 1
  Risk Scores: Financial: 10.223999999999998, Safety: 2.13, Privacy: 2.13
  Risk Factors: exposure: 0.50, complexity: 0.60, attack_surface: 0.70
  Description: An adversary exploits the inherent functionalities of a web browser, in order to establish an unnoticed remote desktop connection in the victim's browser to the adversary's system. The adversary must ...

- Manipulating State
  Impact Scores: Financial: 1.2, Safety: 1, Privacy: 4.8
  Risk Scores: Financial: 2.5559999999999996, Safety: 2.13, Privacy: 10.223999999999998
  Risk Factors: exposure: 0.50, complexity: 0.60, attack_surface: 0.70
  Description: The adversary modifies state information maintained by the target software or causes a state transition in hardware. If successful, the target will use this tainted state and execute in an unintended ...

- Interface Manipulation
  Impact Scores: Financial: 3.5999999999999996, Safety: 1, Privacy: 1
  Risk Scores: Financial: 7.667999999999999, Safety: 2.13, Privacy: 2.13
  Risk Factors: exposure: 0.50, complexity: 0.60, attack_surface: 0.70
  Description: An adversary manipulates the use or processing of an interface (e.g. Application Programming Interface (API) or System-on-Chip (SoC)) resulting in an adverse impact upon the security of the system imp...

- Parameter Injection
  Impact Scores: Financial: 1, Safety: 1, Privacy: 3.5999999999999996
  Risk Scores: Financial: 2.13, Safety: 2.13, Privacy: 7.667999999999999
  Risk Factors: exposure: 0.50, complexity: 0.60, attack_surface: 0.70
  Description: An adversary manipulates the content of request parameters for the purpose of undermining the security of the target. Some parameter encodings use text characters as separators. For example, parameter...

- Content Spoofing
  Impact Scores: Financial: 3.5999999999999996, Safety: 1, Privacy: 3.5999999999999996
  Risk Scores: Financial: 7.667999999999999, Safety: 2.13, Privacy: 7.667999999999999
  Risk Factors: exposure: 0.50, complexity: 0.60, attack_surface: 0.70
  Description: An adversary modifies content to make it contain something other than what the original content producer intended while keeping the apparent source of the content unchanged. The term content spoofing ...

- Resource Location Spoofing
  Impact Scores: Financial: 1, Safety: 1, Privacy: 3.5999999999999996
  Risk Scores: Financial: 2.13, Safety: 2.13, Privacy: 7.667999999999999
  Risk Factors: exposure: 0.50, complexity: 0.60, attack_surface: 0.70
  Description: An adversary deceives an application or user and convinces them to request a resource from an unintended location. By spoofing the location, the adversary can cause an alternate resource to be used, o...

- Cross-Site Flashing
  Impact Scores: Financial: 3.5999999999999996, Safety: 1, Privacy: 1
  Risk Scores: Financial: 7.667999999999999, Safety: 2.13, Privacy: 2.13
  Risk Factors: exposure: 0.50, complexity: 0.60, attack_surface: 0.70
  Description: An attacker is able to trick the victim into executing a Flash document that passes commands or calls to a

Flash player browser plugin, allowing the attacker to exploit native Flash functionality in t...

- Modification of Registry Run Keys
  Impact Scores: Financial: 1, Safety: 1, Privacy: 3.5999999999999996
  Risk Scores: Financial: 2.13, Safety: 2.13, Privacy: 7.667999999999999
  Risk Factors: exposure: 0.50, complexity: 0.60, attack_surface: 0.70
  Description: An adversary adds a new entry to the run keys in the Windows registry so that an application of their choosing is executed when a user logs in. In this way, the adversary can get their executable to o...

- Using Leading 'Ghost' Character Sequences to Bypass Input Filters
  Impact Scores: Financial: 1, Safety: 1, Privacy: 3.5999999999999996
  Risk Scores: Financial: 2.13, Safety: 2.13, Privacy: 7.667999999999999
  Risk Factors: exposure: 0.50, complexity: 0.60, attack_surface: 0.70
  Description: Some APIs will strip certain leading characters from a string of parameters. An adversary can intentionally introduce leading ghost characters (extra characters that don't affect the validity of the r...

- Manipulate Human Behavior
  Impact Scores: Financial: 1, Safety: 1, Privacy: 3.5999999999999996
  Risk Scores: Financial: 2.13, Safety: 2.13, Privacy: 7.667999999999999
  Risk Factors: exposure: 0.50, complexity: 0.60, attack_surface: 0.70
  Description: An adversary exploits inherent human psychological predisposition to influence a targeted individual or group to solicit information or manipulate the target into performing an action that serves the ...

- Disable Security Software
  Impact Scores: Financial: 3.5999999999999996, Safety: 1, Privacy: 1
  Risk Scores: Financial: 7.667999999999999, Safety: 2.13, Privacy: 2.13
  Risk Factors: exposure: 0.50, complexity: 0.60, attack_surface: 0.70
  Description: An adversary exploits a weakness in access control to disable security tools so that detection does not occur. This can take the form of killing processes, deleting registry keys so that tools do not ...

- Collect Data from Registries
  Impact Scores: Financial: 1, Safety: 1, Privacy: 3.5999999999999996
  Risk Scores: Financial: 2.13, Safety: 2.13, Privacy: 7.667999999999999
  Risk Factors: exposure: 0.50, complexity: 0.60, attack_surface: 0.70
  Description: An adversary exploits a weakness in authorization to gather system-specific data and sensitive information within a registry (e.g., Windows Registry, Mac plist). These contain information about the sy...

- Collect Data from Screen Capture
  Impact Scores: Financial: 1, Safety: 1, Privacy: 3.5999999999999996
  Risk Scores: Financial: 2.13, Safety: 2.13, Privacy: 7.667999999999999
  Risk Factors: exposure: 0.50, complexity: 0.60, attack_surface: 0.70
  Description: An adversary gathers sensitive information by exploiting the system's screen capture functionality. Through screenshots, the adversary aims to see what happens on the screen over the course of an oper...

- Retrieve Data from Decommissioned Devices
  Impact Scores: Financial: 1, Safety: 1.2, Privacy: 3.5999999999999996
  Risk Scores: Financial: 2.13, Safety: 2.5559999999999996, Privacy: 7.667999999999999
  Risk Factors: exposure: 0.50, complexity: 0.60, attack_surface: 0.70
  Description: An adversary obtains decommissioned, recycled, or discarded systems and devices that can include an organization’s intellectual property, employee data, and other types of controlled information. Syst...

- ECU Firmware Tampering
  Impact Scores: Financial: 4.8, Safety: 5, Privacy: 3.5999999999999996

Risk Scores: Financial: 6.816, Safety: 7.1, Privacy: 5.111999999999999
Risk Factors: exposure: 0.50, complexity: 0.60, attack_surface: 0.70
Description: Unauthorized modification of ECU firmware causing safety issues...

- Command Line Execution through SQL Injection
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5
  Risk Scores: Financial: 1.42, Safety: 1.42, Privacy: 7.1
  Risk Factors: exposure: 0.50, complexity: 0.60, attack_surface: 0.70
  Description: An attacker uses standard SQL injection methods to inject data into the command line for execution. This could be done directly through misuse of directives such as MSSQL_xp_cmdshell or indirectly thr...

- Escaping a Sandbox by Calling Code in Another Language
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5
  Risk Scores: Financial: 1.42, Safety: 1.42, Privacy: 7.1
  Risk Factors: exposure: 0.50, complexity: 0.60, attack_surface: 0.70
  Description: The attacker may submit malicious code of another language to obtain access to privileges that were not intentionally exposed by the sandbox, thus escaping the sandbox. For instance, Java code cannot ...

- Hijacking a Privileged Thread of Execution
  Impact Scores: Financial: 5, Safety: 1, Privacy: 1
  Risk Scores: Financial: 7.1, Safety: 1.42, Privacy: 1.42
  Risk Factors: exposure: 0.50, complexity: 0.60, attack_surface: 0.70
  Description: An adversary hijacks a privileged thread of execution by injecting malicious code into a running process. By using a privleged thread to do their bidding, adversaries can evade process-based detection...

- Exploitation of Transient Instruction Execution
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5
  Risk Scores: Financial: 1.42, Safety: 1.42, Privacy: 7.1
  Risk Factors: exposure: 0.50, complexity: 0.60, attack_surface: 0.70
  Description: An adversary exploits a hardware design flaw in a CPU implementation of transient instruction execution to expose sensitive data and bypass/subvert access control over restricted resources. Typically,...

- Subvert Code-signing Facilities
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5
  Risk Scores: Financial: 1.42, Safety: 1.42, Privacy: 7.1
  Risk Factors: exposure: 0.50, complexity: 0.60, attack_surface: 0.70
  Description: Many languages use code signing facilities to vouch for code's identity and to thus tie code to its assigned privileges within an environment. Subverting this mechanism can be instrumental in an attac...

- Load Value Injection
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5
  Risk Scores: Financial: 1.42, Safety: 1.42, Privacy: 7.1
  Risk Factors: exposure: 0.50, complexity: 0.60, attack_surface: 0.70
  Description: An adversary exploits a hardware design flaw in a CPU implementation of transient instruction execution in which a faulting or assisted load instruction transiently forwards adversary-controlled data ...

- Web Application Fingerprinting
  Impact Scores: Financial: 1, Safety: 1, Privacy: 2.4
  Risk Scores: Financial: 2.84, Safety: 2.84, Privacy: 6.816
  Risk Factors: exposure: 0.50, complexity: 0.60, attack_surface: 0.70
  Description: An attacker sends a series of probes to a web application in order to elicit version-dependent and type-dependent behavior that assists in identifying the target. An attacker could learn information s...

- Fuzzing for application mapping
  Impact Scores: Financial: 1, Safety: 2.4, Privacy: 1
  Risk Scores: Financial: 2.84, Safety: 6.816, Privacy: 2.84
  Risk Factors: exposure: 0.50, complexity: 0.60, attack_surface: 0.70
  Description: An attacker sends random, malformed, or otherwise unexpected messages to a target application and observes the application's log or error messages returned. The attacker does not initially know how a ...

- Forced Deadlock
  Impact Scores: Financial: 4.8, Safety: 1, Privacy: 1
  Risk Scores: Financial: 6.816, Safety: 1.42, Privacy: 1.42
  Risk Factors: exposure: 0.50, complexity: 0.60, attack_surface: 0.70
  Description: The adversary triggers and exploits a deadlock condition in the target software to cause a denial of service. A deadlock can occur when two or more competing actions are waiting for each other to fini...

- Schema Poisoning
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.8
  Risk Scores: Financial: 1.42, Safety: 1.42, Privacy: 6.816
  Risk Factors: exposure: 0.50, complexity: 0.60, attack_surface: 0.70
  Description: An adversary corrupts or modifies the content of a schema for the purpose of undermining the security of the target. Schemas provide the structure and content definitions for resources used by an appl...

- USB Memory Attacks
  Impact Scores: Financial: 2.4, Safety: 1, Privacy: 4.8
  Risk Scores: Financial: 3.408, Safety: 1.42, Privacy: 6.816
  Risk Factors: exposure: 0.50, complexity: 0.60, attack_surface: 0.70
  Description: An adversary loads malicious code onto a USB memory stick in order to infect any system which the device is plugged in to. USB drives present a significant security risk for business and government ag...

- Signature Spoofing by Misrepresentation
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.8
  Risk Scores: Financial: 1.42, Safety: 1.42, Privacy: 6.816
  Risk Factors: exposure: 0.50, complexity: 0.60, attack_surface: 0.70
  Description: An attacker exploits a weakness in the parsing or display code of the recipient software to generate a data blob containing a supposedly valid signature, but the signer's identity is falsely represent...

- Hardware Component Substitution During Baselining
  Impact Scores: Financial: 4.8, Safety: 1, Privacy: 1
  Risk Scores: Financial: 6.816, Safety: 1.42, Privacy: 1.42
  Risk Factors: exposure: 0.50, complexity: 0.60, attack_surface: 0.70
  Description: An adversary with access to system components during allocated baseline development can substitute a maliciously altered hardware component for a baseline component during the product development and ...

- Malicious Hardware Update
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.8
  Risk Scores: Financial: 1.42, Safety: 1.42, Privacy: 6.816
  Risk Factors: exposure: 0.50, complexity: 0.60, attack_surface: 0.70
  Description: An adversary introduces malicious hardware during an update or replacement procedure, allowing for additional compromise or site disruption at the victim location. After deployment, it is not uncommon...

- Open-Source Library Manipulation
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.8
  Risk Scores: Financial: 1.42, Safety: 1.42, Privacy: 6.816
  Risk Factors: exposure: 0.50, complexity: 0.60, attack_surface: 0.70

Description: Adversaries implant malicious code in open source software (OSS) libraries to have it widely distributed, as OSS is commonly downloaded by developers and other users to incorporate into software devel...

- ASIC With Malicious Functionality
  Impact Scores: Financial: 4.8, Safety: 1, Privacy: 1
  Risk Scores: Financial: 6.816, Safety: 1.42, Privacy: 1.42
  Risk Factors: exposure: 0.50, complexity: 0.60, attack_surface: 0.70
  Description: An attacker with access to the development environment process of an application-specific integrated circuit (ASIC) for a victim system being developed or maintained after initial deployment can inser...

- Replace Trusted Executable
  Impact Scores: Financial: 4.8, Safety: 1, Privacy: 1
  Risk Scores: Financial: 6.816, Safety: 1.42, Privacy: 1.42
  Risk Factors: exposure: 0.50, complexity: 0.60, attack_surface: 0.70
  Description: An adversary exploits weaknesses in privilege management or access control to replace a trusted executable with a malicious version and enable the execution of malware when that trusted executable is ...

- Hardware Fault Injection
  Impact Scores: Financial: 1, Safety: 4.8, Privacy: 4.8
  Risk Scores: Financial: 1.42, Safety: 6.816, Privacy: 6.816
  Risk Factors: exposure: 0.50, complexity: 0.60, attack_surface: 0.70
  Description: The adversary uses disruptive signals or events, or alters the physical environment a device operates in, to cause faulty behavior in electronic devices. This can include electromagnetic pulses, laser...

- Carry-Off GPS Attack
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.8
  Risk Scores: Financial: 1.42, Safety: 1.42, Privacy: 6.816
  Risk Factors: exposure: 0.50, complexity: 0.60, attack_surface: 0.70
  Description: A common form of a GPS spoofing attack, commonly termed a carry-off attack begins with an adversary broadcasting signals synchronized with the genuine signals observed by the target receiver. The powe...

- DLL Side-Loading
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.8
  Risk Scores: Financial: 1.42, Safety: 1.42, Privacy: 6.816
  Risk Factors: exposure: 0.50, complexity: 0.60, attack_surface: 0.70
  Description: An adversary places a malicious version of a Dynamic-Link Library (DLL) in the Windows Side-by-Side (WinSxS) directory to trick the operating system into loading this malicious DLL instead of a legiti...

- Use of Captured Tickets (Pass The Ticket)
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.8
  Risk Scores: Financial: 1.42, Safety: 1.42, Privacy: 6.816
  Risk Factors: exposure: 0.50, complexity: 0.60, attack_surface: 0.70
  Description: An adversary uses stolen Kerberos tickets to access systems/resources that leverage the Kerberos authentication protocol. The Kerberos authentication protocol centers around a ticketing system which i...

- Sniff Application Code
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.8
  Risk Scores: Financial: 1.42, Safety: 1.42, Privacy: 6.816
  Risk Factors: exposure: 0.50, complexity: 0.60, attack_surface: 0.70
  Description: An adversary passively sniffs network communications and captures application code bound for an authorized client. Once obtained, they can use it as-is, or through reverse-engineering glean sensitive ...

- Key Negotiation of Bluetooth Attack (KNOB)

Impact Scores: Financial: 1, Safety: 1, Privacy: 4.8
Risk Scores: Financial: 1.42, Safety: 1.42, Privacy: 6.816
Risk Factors: exposure: 0.50, complexity: 0.60, attack_surface: 0.70
Description: An adversary can exploit a flaw in Bluetooth key negotiation allowing them to decrypt information sent between two devices communicating via Bluetooth. The adversary uses an Adversary in the Middle se...

- Malicious Code Implanted During Chip Programming
  Impact Scores: Financial: 4.8, Safety: 1, Privacy: 1
  Risk Scores: Financial: 6.816, Safety: 1.42, Privacy: 1.42
  Risk Factors: exposure: 0.50, complexity: 0.60, attack_surface: 0.70
  Description: During the programming step of chip manufacture, an adversary with access and necessary technical skills maliciously alters a chip’s intended program logic to produce an effect intended by the adversa...

- AJAX Footprinting
  Impact Scores: Financial: 1, Safety: 1, Privacy: 2.4
  Risk Scores: Financial: 2.84, Safety: 2.84, Privacy: 6.816
  Risk Factors: exposure: 0.50, complexity: 0.60, attack_surface: 0.70
  Description: This attack utilizes the frequent client-server roundtrips in Ajax conversation to scan a system. While Ajax does not open up new vulnerabilities per se, it does optimize them from an attacker point o...

- Interception
  Impact Scores: Financial: 1, Safety: 1, Privacy: 3.5999999999999996
  Risk Scores: Financial: 1.42, Safety: 1.42, Privacy: 5.111999999999999
  Risk Factors: exposure: 0.50, complexity: 0.60, attack_surface: 0.70
  Description: An adversary monitors data streams to or from the target for information gathering purposes. This attack may be undertaken to solely gather sensitive information or to support a further attack against...

- XML Ping of the Death
  Impact Scores: Financial: 1, Safety: 3.5999999999999996, Privacy: 1
  Risk Scores: Financial: 1.42, Safety: 5.111999999999999, Privacy: 1.42
  Risk Factors: exposure: 0.50, complexity: 0.60, attack_surface: 0.70
  Description: An attacker initiates a resource depletion attack where a large number of small XML messages are delivered at a sufficiently rapid rate to cause a denial of service or crash of the target. Transaction...

- Active OS Fingerprinting
  Impact Scores: Financial: 1, Safety: 1, Privacy: 2.4
  Risk Scores: Financial: 2.13, Safety: 2.13, Privacy: 5.111999999999999
  Risk Factors: exposure: 0.50, complexity: 0.60, attack_surface: 0.70
  Description: An adversary engages in activity to detect the operating system or firmware version of a remote target by interrogating a device, server, or platform with a probe designed to solicit behavior that wil...

- TCP Timestamp Probe
  Impact Scores: Financial: 2.4, Safety: 1, Privacy: 1
  Risk Scores: Financial: 5.111999999999999, Safety: 2.13, Privacy: 2.13
  Risk Factors: exposure: 0.50, complexity: 0.60, attack_surface: 0.70
  Description: This OS fingerprinting probe examines the remote server's implementation of TCP timestamps. Not all operating systems implement timestamps within the TCP header, but when timestamps are used then this...

- TCP Sequence Number Probe
  Impact Scores: Financial: 2.4, Safety: 1, Privacy: 1
  Risk Scores: Financial: 5.111999999999999, Safety: 2.13, Privacy: 2.13
  Risk Factors: exposure: 0.50, complexity: 0.60, attack_surface: 0.70
  Description: This OS fingerprinting probe tests the target system's assignment of TCP sequence numbers. One

common way to test TCP Sequence Number generation is to send a probe packet to an open port on the target...

- TCP (ISN) Greatest Common Divisor Probe
  Impact Scores: Financial: 1, Safety: 1, Privacy: 2.4
  Risk Scores: Financial: 2.13, Safety: 2.13, Privacy: 5.111999999999999
  Risk Factors: exposure: 0.50, complexity: 0.60, attack_surface: 0.70
  Description: This OS fingerprinting probe sends a number of TCP SYN packets to an open port of a remote machine. The Initial Sequence Number (ISN) in each of the SYN/ACK response packets is analyzed to determine t...

- TCP (ISN) Counter Rate Probe
  Impact Scores: Financial: 1, Safety: 1, Privacy: 2.4
  Risk Scores: Financial: 2.13, Safety: 2.13, Privacy: 5.111999999999999
  Risk Factors: exposure: 0.50, complexity: 0.60, attack_surface: 0.70
  Description: This OS detection probe measures the average rate of initial sequence number increments during a period of time. Sequence numbers are incremented using a time-based algorithm and are susceptible to a ...

- TCP (ISN) Sequence Predictability Probe
  Impact Scores: Financial: 1, Safety: 1, Privacy: 2.4
  Risk Scores: Financial: 2.13, Safety: 2.13, Privacy: 5.111999999999999
  Risk Factors: exposure: 0.50, complexity: 0.60, attack_surface: 0.70
  Description: This type of operating system probe attempts to determine an estimate for how predictable the sequence number generation algorithm is for a remote host. Statistical techniques, such as standard deviat...

- TCP Initial Window Size Probe
  Impact Scores: Financial: 2.4, Safety: 1, Privacy: 1
  Risk Scores: Financial: 5.111999999999999, Safety: 2.13, Privacy: 2.13
  Risk Factors: exposure: 0.50, complexity: 0.60, attack_surface: 0.70
  Description: This OS fingerprinting probe checks the initial TCP Window size. TCP stacks limit the range of sequence numbers allowable within a session to maintain the connected state within TCP protocol logic. Th...

- TCP Options Probe
  Impact Scores: Financial: 2.4, Safety: 1, Privacy: 1
  Risk Scores: Financial: 5.111999999999999, Safety: 2.13, Privacy: 2.13
  Risk Factors: exposure: 0.50, complexity: 0.60, attack_surface: 0.70
  Description: This OS fingerprinting probe analyzes the type and order of any TCP header options present within a response segment. Most operating systems use unique ordering and different option sets when options ...

- Pretexting
  Impact Scores: Financial: 1, Safety: 1, Privacy: 2.4
  Risk Scores: Financial: 2.13, Safety: 2.13, Privacy: 5.111999999999999
  Risk Factors: exposure: 0.50, complexity: 0.60, attack_surface: 0.70
  Description: An adversary engages in pretexting behavior to solicit information from target persons, or manipulate the target into performing some action that serves the adversary's interests. During a pretexting ...

- Incomplete Data Deletion in a Multi-Tenant Environment
  Impact Scores: Financial: 1, Safety: 1, Privacy: 3.5999999999999996
  Risk Scores: Financial: 1.42, Safety: 1.42, Privacy: 5.111999999999999
  Risk Factors: exposure: 0.50, complexity: 0.60, attack_surface: 0.70
  Description: An adversary obtains unauthorized information due to insecure or incomplete data deletion in a multi-tenant environment. If a cloud provider fails to completely delete storage and data from former clo...

- Adding a Space to a File Extension
  Impact Scores: Financial: 1, Safety: 1, Privacy: 3.5999999999999996

Risk Scores: Financial: 1.42, Safety: 1.42, Privacy: 5.111999999999999
Risk Factors: exposure: 0.50, complexity: 0.60, attack_surface: 0.70
Description: An adversary adds a space character to the end of a file extension and takes advantage of an application that does not properly neutralize trailing special elements in file names. This extra space, wh...

- Reverse Engineering
  Impact Scores: Financial: 2.4, Safety: 1, Privacy: 1
  Risk Scores: Financial: 3.408, Safety: 1.42, Privacy: 1.42
  Risk Factors: exposure: 0.50, complexity: 0.60, attack_surface: 0.70
  Description: An adversary discovers the structure, function, and composition of an object, resource, or system by using a variety of analysis techniques to effectively determine how the analyzed entity was constru...

- Fingerprinting
  Impact Scores: Financial: 1, Safety: 1, Privacy: 1.2
  Risk Scores: Financial: 2.84, Safety: 2.84, Privacy: 3.408
  Risk Factors: exposure: 0.50, complexity: 0.60, attack_surface: 0.70
  Description: An adversary compares output from a target system to known indicators that uniquely identify specific details about the target. Most commonly, fingerprinting is done to determine operating system and ...

- Target Influence via Framing
  Impact Scores: Financial: 1, Safety: 1.2, Privacy: 2.4
  Risk Scores: Financial: 1.42, Safety: 1.704, Privacy: 3.408
  Risk Factors: exposure: 0.50, complexity: 0.60, attack_surface: 0.70
  Description: An adversary uses framing techniques to contextualize a conversation so that the target is more likely to be influenced by the adversary's point of view. Framing is information and experiences in life...

- Influence via Psychological Principles
  Impact Scores: Financial: 2.4, Safety: 1, Privacy: 1
  Risk Scores: Financial: 3.408, Safety: 1.42, Privacy: 1.42
  Risk Factors: exposure: 0.50, complexity: 0.60, attack_surface: 0.70
  Description: The adversary shapes the target's actions or behavior by focusing on the ways human interact and learn, leveraging such elements as cognitive and social psychology. In a variety of ways, a target can ...

- Process Footprinting
  Impact Scores: Financial: 1, Safety: 1, Privacy: 2.4
  Risk Scores: Financial: 1.42, Safety: 1.42, Privacy: 3.408
  Risk Factors: exposure: 0.50, complexity: 0.60, attack_surface: 0.70
  Description: An adversary exploits functionality meant to identify information about the currently running processes on the target system to an authorized user. By knowing what processes are running on the target ...

- Services Footprinting
  Impact Scores: Financial: 1, Safety: 1, Privacy: 2.4
  Risk Scores: Financial: 1.42, Safety: 1.42, Privacy: 3.408
  Risk Factors: exposure: 0.50, complexity: 0.60, attack_surface: 0.70
  Description: An adversary exploits functionality meant to identify information about the services on the target system to an authorized user. By knowing what services are registered on the target system, the adver...

- Account Footprinting
  Impact Scores: Financial: 1, Safety: 1, Privacy: 2.4
  Risk Scores: Financial: 1.42, Safety: 1.42, Privacy: 3.408
  Risk Factors: exposure: 0.50, complexity: 0.60, attack_surface: 0.70
  Description: An adversary exploits functionality meant to identify information about the domain accounts and their permissions on the target system to an authorized user. By knowing what accounts are registered on...

- Group Permission Footprinting
  Impact Scores: Financial: 1, Safety: 1, Privacy: 2.4
  Risk Scores: Financial: 1.42, Safety: 1.42, Privacy: 3.408
  Risk Factors: exposure: 0.50, complexity: 0.60, attack_surface: 0.70
  Description: An adversary exploits functionality meant to identify information about user groups and their permissions on the target system to an authorized user. By knowing what users/permissions are registered o...

- Owner Footprinting
  Impact Scores: Financial: 1, Safety: 1, Privacy: 2.4
  Risk Scores: Financial: 1.42, Safety: 1.42, Privacy: 3.408
  Risk Factors: exposure: 0.50, complexity: 0.60, attack_surface: 0.70
  Description: An adversary exploits functionality meant to identify information about the primary users on the target system to an authorized user. They may do this, for example, by reviewing logins or file modific...

- System Footprinting
  Impact Scores: Financial: 1, Safety: 1, Privacy: 2.4
  Risk Scores: Financial: 1.42, Safety: 1.42, Privacy: 3.408
  Risk Factors: exposure: 0.50, complexity: 0.60, attack_surface: 0.70
  Description: An adversary engages in active probing and exploration activities to determine security information about a remote target system. Often times adversaries will rely on remote applications that can be p...

- Collect Data from Clipboard
  Impact Scores: Financial: 1, Safety: 1, Privacy: 2.4
  Risk Scores: Financial: 1.42, Safety: 1.42, Privacy: 3.408
  Risk Factors: exposure: 0.50, complexity: 0.60, attack_surface: 0.70
  Description: The adversary exploits an application that allows for the copying of sensitive data or information by collecting information copied to the clipboard. Data copied to the clipboard can be accessed by ot...

Component: Brake Control Unit

Type: ECU
Safety Level: ASIL D
Interfaces: CAN
Access Points: Debug Port
Data Types: Sensor Data, Control Commands
Location: Internal
Trust Zone: Critical
Connected To: ECU001, SNS002, ECU002

Identified Threats:

- Accessing Functionality Not Properly Constrained by ACLs
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5
  Risk Scores: Financial: 2.84, Safety: 2.84, Privacy: 14.2
  Risk Factors: exposure: 0.50, complexity: 0.50, attack_surface: 0.70
  Description: In applications, particularly web applications, access to functionality is mitigated by an authorization framework. This framework maps Access Control Lists (ACLs) to elements of the application's fun...

- Buffer Overflow via Environment Variables
  Impact Scores: Financial: 5, Safety: 1, Privacy: 1
  Risk Scores: Financial: 14.2, Safety: 2.84, Privacy: 2.84

Risk Factors: exposure: 0.50, complexity: 0.50, attack_surface: 0.70

Description: This attack pattern involves causing a buffer overflow through manipulation of environment variables. Once the adversary finds that they can modify an environment variable, they may try to overflow as...

- Server Side Include (SSI) Injection
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5
  Risk Scores: Financial: 2.84, Safety: 2.84, Privacy: 14.2
  Risk Factors: exposure: 0.50, complexity: 0.50, attack_surface: 0.70
  Description: An attacker can use Server Side Include (SSI) Injection to send code to a web application that then gets executed by the web server. Doing so enables the attacker to achieve similar results to Cross S...

- Buffer Manipulation
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5
  Risk Scores: Financial: 2.84, Safety: 2.84, Privacy: 14.2
  Risk Factors: exposure: 0.50, complexity: 0.50, attack_surface: 0.70
  Description: An adversary manipulates an application's interaction with a buffer in an attempt to read or modify data they shouldn't have access to. Buffer attacks are distinguished in that it is the buffer space ...

- Format String Injection
  Impact Scores: Financial: 1, Safety: 2.8, Privacy: 5
  Risk Scores: Financial: 2.84, Safety: 7.951999999999999, Privacy: 14.2
  Risk Factors: exposure: 0.50, complexity: 0.50, attack_surface: 0.70
  Description: An adversary includes formatting characters in a string input field on the target application. Most applications assume that users will provide static text and may respond unpredictably to the presenc...

- Cache Poisoning
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5
  Risk Scores: Financial: 2.84, Safety: 2.84, Privacy: 14.2
  Risk Factors: exposure: 0.50, complexity: 0.50, attack_surface: 0.70
  Description: An attacker exploits the functionality of cache technologies to cause specific data to be cached that aids the attackers' objectives. This describes any attack whereby an attacker places incorrect or ...

- DNS Cache Poisoning
  Impact Scores: Financial: 5, Safety: 1, Privacy: 1
  Risk Scores: Financial: 14.2, Safety: 2.84, Privacy: 2.84
  Risk Factors: exposure: 0.50, complexity: 0.50, attack_surface: 0.70
  Description: A domain name server translates a domain name (such as www.example.com) into an IP address that Internet hosts use to contact Internet resources. An adversary modifies a public DNS cache to cause cert...

- Command Delimiters
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5
  Risk Scores: Financial: 2.84, Safety: 2.84, Privacy: 14.2
  Risk Factors: exposure: 0.50, complexity: 0.50, attack_surface: 0.70
  Description: An attack of this type exploits a programs' vulnerabilities that allows an attacker's commands to be concatenated onto a legitimate command with the intent of targeting other resources such as the fil...

- Redirect Access to Libraries
  Impact Scores: Financial: 1, Safety: 5, Privacy: 1
  Risk Scores: Financial: 2.84, Safety: 14.2, Privacy: 2.84
  Risk Factors: exposure: 0.50, complexity: 0.50, attack_surface: 0.70
  Description: An adversary exploits a weakness in the way an application searches for external libraries to manipulate the execution flow to point to an adversary supplied library or code base. This pattern of atta...

- XSS Targeting Non-Script Elements
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5
  Risk Scores: Financial: 2.84, Safety: 2.84, Privacy: 14.2
  Risk Factors: exposure: 0.50, complexity: 0.50, attack_surface: 0.70
  Description: This attack is a form of Cross-Site Scripting (XSS) where malicious scripts are embedded in elements that are not expected to host scripts such as image tags (<img>), comments in XML documents (< !-CD...

- Malicious Automated Software Update via Redirection
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5
  Risk Scores: Financial: 2.84, Safety: 2.84, Privacy: 14.2
  Risk Factors: exposure: 0.50, complexity: 0.50, attack_surface: 0.70
  Description: An attacker exploits two layers of weaknesses in server or client software for automated update mechanisms to undermine the integrity of the target code-base. The first weakness involves a failure to ...

- PHP Remote File Inclusion
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5
  Risk Scores: Financial: 2.84, Safety: 2.84, Privacy: 14.2
  Risk Factors: exposure: 0.50, complexity: 0.50, attack_surface: 0.70
  Description: In this pattern the adversary is able to load and execute arbitrary code remotely available from the application. This is usually accomplished through an insecurely configured PHP runtime environment ...

- XSS Using Alternate Syntax
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5
  Risk Scores: Financial: 2.84, Safety: 2.84, Privacy: 14.2
  Risk Factors: exposure: 0.50, complexity: 0.50, attack_surface: 0.70
  Description: An adversary uses alternate forms of keywords or commands that result in the same action as the primary form but which may not be caught by filters. For example, many keywords are processed in a case ...

- Serialized Data External Linking
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5
  Risk Scores: Financial: 2.84, Safety: 2.84, Privacy: 14.2
  Risk Factors: exposure: 0.50, complexity: 0.50, attack_surface: 0.70
  Description: An adversary creates a serialized data file (e.g. XML, YAML, etc...) that contains an external data reference. Because serialized data parsers may not validate documents with external references, ther...

- Leveraging Race Conditions
  Impact Scores: Financial: 5, Safety: 1, Privacy: 1
  Risk Scores: Financial: 14.2, Safety: 2.84, Privacy: 2.84
  Risk Factors: exposure: 0.50, complexity: 0.50, attack_surface: 0.70
  Description: The adversary targets a race condition occurring when multiple processes access and manipulate the same resource concurrently, and the outcome of the execution depends on the particular order in which...

- Leveraging Time-of-Check and Time-of-Use (TOCTOU) Race Conditions
  Impact Scores: Financial: 5, Safety: 1, Privacy: 1
  Risk Scores: Financial: 14.2, Safety: 2.84, Privacy: 2.84
  Risk Factors: exposure: 0.50, complexity: 0.50, attack_surface: 0.70
  Description: This attack targets a race condition occurring between the time of check (state) for a resource and the time of use of a resource. A typical example is file access. The adversary can leverage a file a...

- Leverage Executable Code in Non-Executable Files
  Impact Scores: Financial: 5, Safety: 1, Privacy: 1
  Risk Scores: Financial: 14.2, Safety: 2.84, Privacy: 2.84
  Risk Factors: exposure: 0.50, complexity: 0.50, attack_surface: 0.70

Description: An attack of this type exploits a system's trust in configuration and resource files. When the executable loads the resource (such as an image file or configuration file) the attacker has modified the...

- Retrieve Embedded Sensitive Data
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5
  Risk Scores: Financial: 2.84, Safety: 2.84, Privacy: 14.2
  Risk Factors: exposure: 0.50, complexity: 0.50, attack_surface: 0.70
  Description: An attacker examines a target system to find sensitive data that has been embedded within it. This information can reveal confidential contents, such as account numbers or individual keys/credentials ...

- Leveraging/Manipulating Configuration File Search Paths
  Impact Scores: Financial: 5, Safety: 1, Privacy: 1
  Risk Scores: Financial: 14.2, Safety: 2.84, Privacy: 2.84
  Risk Factors: exposure: 0.50, complexity: 0.50, attack_surface: 0.70
  Description: This pattern of attack sees an adversary load a malicious resource into a program's standard path so that when a known command is executed then the system instead executes the malicious component. The...

- Manipulating Writeable Terminal Devices
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5
  Risk Scores: Financial: 2.84, Safety: 2.84, Privacy: 14.2
  Risk Factors: exposure: 0.50, complexity: 0.50, attack_surface: 0.70
  Description: This attack exploits terminal devices that allow themselves to be written to by other users. The attacker sends command strings to the target terminal device hoping that the target user will hit enter...

- Using Meta-characters in E-mail Headers to Inject Malicious Payloads
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5
  Risk Scores: Financial: 2.84, Safety: 2.84, Privacy: 14.2
  Risk Factors: exposure: 0.50, complexity: 0.50, attack_surface: 0.70
  Description: This type of attack involves an attacker leveraging meta-characters in email headers to inject improper behavior into email programs. Email software has become increasingly sophisticated and feature-r...

- Overflow Binary Resource File
  Impact Scores: Financial: 5, Safety: 1, Privacy: 1
  Risk Scores: Financial: 14.2, Safety: 2.84, Privacy: 2.84
  Risk Factors: exposure: 0.50, complexity: 0.50, attack_surface: 0.70
  Description: An attack of this type exploits a buffer overflow vulnerability in the handling of binary resources. Binary resources may include music files like MP3, image files like JPEG files, and any other binar...

- Buffer Overflow via Symbolic Links
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5
  Risk Scores: Financial: 2.84, Safety: 2.84, Privacy: 14.2
  Risk Factors: exposure: 0.50, complexity: 0.50, attack_surface: 0.70
  Description: This type of attack leverages the use of symbolic links to cause buffer overflows. An adversary can try to create or manipulate a symbolic link file such that its contents result in out of bounds data...

- Passing Local Filenames to Functions That Expect a URL
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5
  Risk Scores: Financial: 2.84, Safety: 2.84, Privacy: 14.2
  Risk Factors: exposure: 0.50, complexity: 0.50, attack_surface: 0.70
  Description: This attack relies on client side code to access local files and resources instead of URLs. When the client browser is expecting a URL string, but instead receives a request for a local file, that exe...

- Poison Web Service Registry

Impact Scores: Financial: 1, Safety: 1, Privacy: 5
Risk Scores: Financial: 2.84, Safety: 2.84, Privacy: 14.2
Risk Factors: exposure: 0.50, complexity: 0.50, attack_surface: 0.70
Description: SOA and Web Services often use a registry to perform look up, get schema information, and metadata about services. A poisoned registry can redirect (think phishing for servers) the service requester t...

- Session Credential Falsification through Prediction
  Impact Scores: Financial: 5, Safety: 1, Privacy: 1
  Risk Scores: Financial: 14.2, Safety: 2.84, Privacy: 2.84
  Risk Factors: exposure: 0.50, complexity: 0.50, attack_surface: 0.70
  Description: This attack targets predictable session ID in order to gain privileges. The attacker can predict the session ID used during a transaction to perform spoofing and session hijacking....

- Using Slashes and URL Encoding Combined to Bypass Validation Logic
  Impact Scores: Financial: 5, Safety: 1, Privacy: 1
  Risk Scores: Financial: 14.2, Safety: 2.84, Privacy: 2.84
  Risk Factors: exposure: 0.50, complexity: 0.50, attack_surface: 0.70
  Description: This attack targets the encoding of the URL combined with the encoding of the slash characters. An attacker can take advantage of the multiple ways of encoding a URL and abuse the interpretation of th...

- Avoid Security Tool Identification by Adding Data
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5
  Risk Scores: Financial: 2.84, Safety: 2.84, Privacy: 14.2
  Risk Factors: exposure: 0.50, complexity: 0.50, attack_surface: 0.70
  Description: An adversary adds data to a file to increase the file size beyond what security tools are capable of handling in an attempt to mask their actions. In addition to this, adding data to a file also chang...

- Voice Phishing
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5
  Risk Scores: Financial: 2.84, Safety: 2.84, Privacy: 14.2
  Risk Factors: exposure: 0.50, complexity: 0.50, attack_surface: 0.70
  Description: An adversary targets users with a phishing attack for the purpose of soliciting account passwords or sensitive information from the user. Voice Phishing is a variation of the Phishing social engineeri...

- Malicious Automated Software Update via Spoofing
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5
  Risk Scores: Financial: 2.84, Safety: 2.84, Privacy: 14.2
  Risk Factors: exposure: 0.50, complexity: 0.50, attack_surface: 0.70
  Description: An attackers uses identify or content spoofing to trick a client into performing an automated software update from a malicious source. A malicious automated software update that leverages spoofing can...

- String Format Overflow in syslog()
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5
  Risk Scores: Financial: 2.84, Safety: 2.84, Privacy: 14.2
  Risk Factors: exposure: 0.50, complexity: 0.50, attack_surface: 0.70
  Description: This attack targets applications and software that uses the syslog() function insecurely. If an application does not explicitely use a format string parameter in a call to syslog(), user input can be ...

- Blind SQL Injection
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5
  Risk Scores: Financial: 2.84, Safety: 2.84, Privacy: 14.2
  Risk Factors: exposure: 0.50, complexity: 0.50, attack_surface: 0.70
  Description: Blind SQL Injection results from an insufficient mitigation for SQL Injection. Although suppressing

database error messages are considered best practice, the suppression alone is not sufficient to pre...

- URL Encoding
  Impact Scores: Financial: 5, Safety: 1, Privacy: 1
  Risk Scores: Financial: 14.2, Safety: 2.84, Privacy: 2.84
  Risk Factors: exposure: 0.50, complexity: 0.50, attack_surface: 0.70
  Description: This attack targets the encoding of the URL. An adversary can take advantage of the multiple way of encoding an URL and abuse the interpretation of the URL....

- User-Controlled Filename
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5
  Risk Scores: Financial: 2.84, Safety: 2.84, Privacy: 14.2
  Risk Factors: exposure: 0.50, complexity: 0.50, attack_surface: 0.70
  Description: An attack of this type involves an adversary inserting malicious characters (such as a XSS redirection) into a filename, directly or indirectly that is then used by the target software to generate HTM...

- Manipulating User-Controlled Variables
  Impact Scores: Financial: 2.8, Safety: 1, Privacy: 5
  Risk Scores: Financial: 7.951999999999999, Safety: 2.84, Privacy: 14.2
  Risk Factors: exposure: 0.50, complexity: 0.50, attack_surface: 0.70
  Description: This attack targets user controlled variables (DEBUG=1, PHP Globals, and So Forth). An adversary can override variables leveraging user-supplied, untrusted query variables directly used on the applica...

- Using Escaped Slashes in Alternate Encoding
  Impact Scores: Financial: 5, Safety: 1, Privacy: 1
  Risk Scores: Financial: 14.2, Safety: 2.84, Privacy: 2.84
  Risk Factors: exposure: 0.50, complexity: 0.50, attack_surface: 0.70
  Description: This attack targets the use of the backslash in alternate encoding. An adversary can provide a backslash as a leading character and causes a parser to believe that the next character is special. This ...

- Buffer Overflow in an API Call
  Impact Scores: Financial: 5, Safety: 1, Privacy: 1
  Risk Scores: Financial: 14.2, Safety: 2.84, Privacy: 2.84
  Risk Factors: exposure: 0.50, complexity: 0.50, attack_surface: 0.70
  Description: This attack targets libraries or shared code modules which are vulnerable to buffer overflow attacks. An adversary who has knowledge of known vulnerable libraries or shared code can easily target soft...

- Using UTF-8 Encoding to Bypass Validation Logic
  Impact Scores: Financial: 1, Safety: 5, Privacy: 1
  Risk Scores: Financial: 2.84, Safety: 14.2, Privacy: 2.84
  Risk Factors: exposure: 0.50, complexity: 0.50, attack_surface: 0.70
  Description: This attack is a specific variation on leveraging alternate encodings to bypass validation logic. This attack leverages the possibility to encode potentially harmful input in UTF-8 and submit it to ap...

- XPath Injection
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5
  Risk Scores: Financial: 2.84, Safety: 2.84, Privacy: 14.2
  Risk Factors: exposure: 0.50, complexity: 0.50, attack_surface: 0.70
  Description: An attacker can craft special user-controllable input consisting of XPath expressions to inject the XML database and bypass authentication or glean information that they normally would not be able to....

- XQuery Injection
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5

Risk Scores: Financial: 2.84, Safety: 2.84, Privacy: 14.2
Risk Factors: exposure: 0.50, complexity: 0.50, attack_surface: 0.70
Description: This attack utilizes XQuery to probe and attack server systems; in a similar manner that SQL Injection allows an attacker to exploit SQL calls to RDBMS, XQuery Injection uses improperly validated data...

- OS Command Injection
  Impact Scores: Financial: 5, Safety: 1, Privacy: 1
  Risk Scores: Financial: 14.2, Safety: 2.84, Privacy: 2.84
  Risk Factors: exposure: 0.50, complexity: 0.50, attack_surface: 0.70
  Description: In this type of an attack, an adversary injects operating system commands into existing application functions. An application that uses untrusted input to build command strings is vulnerable. An adver...

- Pharming
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5
  Risk Scores: Financial: 2.84, Safety: 2.84, Privacy: 14.2
  Risk Factors: exposure: 0.50, complexity: 0.50, attack_surface: 0.70
  Description: A pharming attack occurs when the victim is fooled into entering sensitive data into supposedly trusted locations, such as an online bank site or a trading platform. An attacker can impersonate these ...

- Buffer Overflow in Local Command-Line Utilities
  Impact Scores: Financial: 5, Safety: 1, Privacy: 1
  Risk Scores: Financial: 14.2, Safety: 2.84, Privacy: 2.84
  Risk Factors: exposure: 0.50, complexity: 0.50, attack_surface: 0.70
  Description: This attack targets command-line utilities available in a number of shells. An adversary can leverage a vulnerability found in a command-line utility to escalate privilege to root....

- Reflection Attack in Authentication Protocol
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5
  Risk Scores: Financial: 2.84, Safety: 2.84, Privacy: 14.2
  Risk Factors: exposure: 0.50, complexity: 0.50, attack_surface: 0.70
  Description: An adversary can abuse an authentication protocol susceptible to reflection attack in order to defeat it. Doing so allows the adversary illegitimate access to the target system, without possessing the...

- Forced Integer Overflow
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5
  Risk Scores: Financial: 2.84, Safety: 2.84, Privacy: 14.2
  Risk Factors: exposure: 0.50, complexity: 0.50, attack_surface: 0.70
  Description: This attack forces an integer variable to go out of range. The integer variable is often used as an offset such as size of memory allocation or similarly. The attacker would typically control the valu...

- WSDL Scanning
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5
  Risk Scores: Financial: 2.84, Safety: 2.84, Privacy: 14.2
  Risk Factors: exposure: 0.50, complexity: 0.50, attack_surface: 0.70
  Description: This attack targets the WSDL interface made available by a web service. The attacker may scan the WSDL interface to reveal sensitive information about invocation patterns, underlying technology implem...

- Phishing
  Impact Scores: Financial: 1.4, Safety: 1, Privacy: 5
  Risk Scores: Financial: 3.9759999999999995, Safety: 2.84, Privacy: 14.2
  Risk Factors: exposure: 0.50, complexity: 0.50, attack_surface: 0.70
  Description: Phishing is a social engineering technique where an attacker masquerades as a legitimate entity with which the victim might do business in order to prompt the user to reveal some confidential informat...

- Flooding
  Impact Scores: Financial: 1, Safety: 1.4, Privacy: 4.199999999999999
  Risk Scores: Financial: 2.84, Safety: 3.9759999999999995, Privacy: 11.927999999999997
  Risk Factors: exposure: 0.50, complexity: 0.50, attack_surface: 0.70
  Description: An adversary consumes the resources of a target by rapidly engaging in a large number of interactions with the target. This type of attack generally exposes a weakness in rate limiting or flow. When s...

- Directory Indexing
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.199999999999999
  Risk Scores: Financial: 2.84, Safety: 2.84, Privacy: 11.927999999999997
  Risk Factors: exposure: 0.50, complexity: 0.50, attack_surface: 0.70
  Description: An adversary crafts a request to a target that results in the target listing/indexing the content of a directory as output. One common method of triggering directory contents as output is to construct...

- Flash Parameter Injection
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.199999999999999
  Risk Scores: Financial: 2.84, Safety: 2.84, Privacy: 11.927999999999997
  Risk Factors: exposure: 0.50, complexity: 0.50, attack_surface: 0.70
  Description: An adversary takes advantage of improper data validation to inject malicious global parameters into a Flash file embedded within an HTML document. Flash files can leverage user-submitted data to confi...

- Exploiting Incorrectly Configured Access Control Security Levels
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.199999999999999
  Risk Scores: Financial: 2.84, Safety: 2.84, Privacy: 11.927999999999997
  Risk Factors: exposure: 0.50, complexity: 0.50, attack_surface: 0.70
  Description: An attacker exploits a weakness in the configuration of access controls and is able to bypass the intended protection that these measures guard against and thereby obtain unauthorized access to the sy...

- Exponential Data Expansion
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.199999999999999
  Risk Scores: Financial: 2.84, Safety: 2.84, Privacy: 11.927999999999997
  Risk Factors: exposure: 0.50, complexity: 0.50, attack_surface: 0.70
  Description: An adversary submits data to a target application which contains nested exponential data expansion to produce excessively large output. Many data format languages allow the definition of macro-like st...

- Inducing Account Lockout
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.199999999999999
  Risk Scores: Financial: 2.84, Safety: 2.84, Privacy: 11.927999999999997
  Risk Factors: exposure: 0.50, complexity: 0.50, attack_surface: 0.70
  Description: An attacker leverages the security functionality of the system aimed at thwarting potential attacks to launch a denial of service attack against a legitimate system user. Many systems, for instance, i...

- XML Routing Detour Attacks
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.199999999999999
  Risk Scores: Financial: 2.84, Safety: 2.84, Privacy: 11.927999999999997
  Risk Factors: exposure: 0.50, complexity: 0.50, attack_surface: 0.70
  Description: An attacker subverts an intermediate system used to process XML content and forces the intermediate to modify and/or re-route the processing of the content. XML Routing Detour Attacks are Adversary in...

- Fuzzing
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.199999999999999
  Risk Scores: Financial: 2.84, Safety: 2.84, Privacy: 11.927999999999997
  Risk Factors: exposure: 0.50, complexity: 0.50, attack_surface: 0.70

Description: In this attack pattern, the adversary leverages fuzzing to try to identify weaknesses in the system. Fuzzing is a software security and functionality testing method that feeds randomly constructed inp...

- Manipulating Opaque Client-based Data Tokens
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.199999999999999
  Risk Scores: Financial: 2.84, Safety: 2.84, Privacy: 11.927999999999997
  Risk Factors: exposure: 0.50, complexity: 0.50, attack_surface: 0.70
  Description: In circumstances where an application holds important data client-side in tokens (cookies, URLs, data files, and so forth) that data can be manipulated. If client or server-side application components...

- CAN Injection
  Impact Scores: Financial: 4.199999999999999, Safety: 5, Privacy: 2.8
  Risk Scores: Financial: 8.945999999999998, Safety: 10.649999999999999, Privacy: 5.9639999999999995
  Risk Factors: exposure: 0.50, complexity: 0.50, attack_surface: 0.70
  Description: Manipulation of CAN bus messages leading to vehicle malfunction...

- Sensor Data Manipulation
  Impact Scores: Financial: 4.199999999999999, Safety: 5, Privacy: 2.8
  Risk Scores: Financial: 8.945999999999998, Safety: 10.649999999999999, Privacy: 5.9639999999999995
  Risk Factors: exposure: 0.50, complexity: 0.50, attack_surface: 0.70
  Description: Tampering with sensor data leading to incorrect vehicle behavior...

- HTTP Request Splitting
  Impact Scores: Financial: 5, Safety: 1, Privacy: 1
  Risk Scores: Financial: 10.649999999999999, Safety: 2.13, Privacy: 2.13
  Risk Factors: exposure: 0.50, complexity: 0.50, attack_surface: 0.70
  Description: An adversary abuses the flexibility and discrepancies in the parsing and interpretation of HTTP Request messages by different intermediary HTTP agents (e.g., load balancer, reverse proxy, web caching ...

- Serialized Data with Nested Payloads
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5
  Risk Scores: Financial: 2.13, Safety: 2.13, Privacy: 10.649999999999999
  Risk Factors: exposure: 0.50, complexity: 0.50, attack_surface: 0.70
  Description: Applications often need to transform data in and out of a data format (e.g., XML and YAML) by using a parser. It may be possible for an adversary to inject data that may have an adverse effect on the ...

- Command Injection
  Impact Scores: Financial: 5, Safety: 1, Privacy: 1
  Risk Scores: Financial: 10.649999999999999, Safety: 2.13, Privacy: 2.13
  Risk Factors: exposure: 0.50, complexity: 0.50, attack_surface: 0.70
  Description: An adversary looking to execute a command of their choosing, injects new items into an existing command thus modifying interpretation away from what was intended. Commands in this context are often st...

- Leveraging Race Conditions via Symbolic Links
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5
  Risk Scores: Financial: 2.13, Safety: 2.13, Privacy: 10.649999999999999
  Risk Factors: exposure: 0.50, complexity: 0.50, attack_surface: 0.70
  Description: This attack leverages the use of symbolic links (Symlinks) in order to write to sensitive files. An attacker can create a Symlink link to a target file not otherwise accessible to them. When the privi...

- HTTP Response Smuggling
  Impact Scores: Financial: 5, Safety: 1, Privacy: 1
  Risk Scores: Financial: 10.649999999999999, Safety: 2.13, Privacy: 2.13

Risk Factors: exposure: 0.50, complexity: 0.50, attack_surface: 0.70
Description: An adversary manipulates and injects malicious content in the form of secret unauthorized HTTP responses, into a single HTTP response from a vulnerable or compromised back-end HTTP agent (e.g., server...

- SOAP Manipulation
  Impact Scores: Financial: 5, Safety: 1, Privacy: 1
  Risk Scores: Financial: 10.649999999999999, Safety: 2.13, Privacy: 2.13
  Risk Factors: exposure: 0.50, complexity: 0.50, attack_surface: 0.70
  Description: Simple Object Access Protocol (SOAP) is used as a communication protocol between a client and server to invoke web services on the server. It is an XML-based protocol, and therefore suffers from many ...

- HTTP Request Smuggling
  Impact Scores: Financial: 5, Safety: 1, Privacy: 1
  Risk Scores: Financial: 10.649999999999999, Safety: 2.13, Privacy: 2.13
  Risk Factors: exposure: 0.50, complexity: 0.50, attack_surface: 0.70
  Description: An adversary abuses the flexibility and discrepancies in the parsing and interpretation of HTTP Request messages using various HTTP headers, request-line and body parameters as well as message sizes (...

- HTTP Response Splitting
  Impact Scores: Financial: 5, Safety: 1, Privacy: 1
  Risk Scores: Financial: 10.649999999999999, Safety: 2.13, Privacy: 2.13
  Risk Factors: exposure: 0.50, complexity: 0.50, attack_surface: 0.70
  Description: An adversary manipulates and injects malicious content, in the form of secret unauthorized HTTP responses, into a single HTTP response from a vulnerable or compromised back-end HTTP agent (e.g., web s...

- Using Alternative IP Address Encodings
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5
  Risk Scores: Financial: 2.13, Safety: 2.13, Privacy: 10.649999999999999
  Risk Factors: exposure: 0.50, complexity: 0.50, attack_surface: 0.70
  Description: This attack relies on the adversary using unexpected formats for representing IP addresses. Networked applications may expect network location information in a specific format, such as fully qualified...

- Exploiting Multiple Input Interpretation Layers
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5
  Risk Scores: Financial: 2.13, Safety: 2.13, Privacy: 10.649999999999999
  Risk Factors: exposure: 0.50, complexity: 0.50, attack_surface: 0.70
  Description: An attacker supplies the target software with input data that contains sequences of special characters designed to bypass input validation logic. This exploit relies on the target making multiples pas...

- Development Alteration
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5
  Risk Scores: Financial: 2.13, Safety: 2.13, Privacy: 10.649999999999999
  Risk Factors: exposure: 0.50, complexity: 0.50, attack_surface: 0.70
  Description: An adversary modifies a technology, product, or component during its development to acheive a negative impact once the system is deployed. The goal of the adversary is to modify the system in such a w...

- Malicious Logic Insertion into Product Software via Configuration Management Manipulation
  Impact Scores: Financial: 5, Safety: 1, Privacy: 1
  Risk Scores: Financial: 10.649999999999999, Safety: 2.13, Privacy: 2.13
  Risk Factors: exposure: 0.50, complexity: 0.50, attack_surface: 0.70
  Description: An adversary exploits a configuration management system so that malicious logic is inserted into a software products build, update or deployed environment. If an adversary can control the elements inc...

- Design Alteration
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5
  Risk Scores: Financial: 2.13, Safety: 2.13, Privacy: 10.649999999999999
  Risk Factors: exposure: 0.50, complexity: 0.50, attack_surface: 0.70
  Description: An adversary modifies the design of a technology, product, or component to acheive a negative impact once the system is deployed. In this type of attack, the goal of the adversary is to modify the des...

- Contradictory Destinations in Traffic Routing Schemes
  Impact Scores: Financial: 5, Safety: 1, Privacy: 1
  Risk Scores: Financial: 10.649999999999999, Safety: 2.13, Privacy: 2.13
  Risk Factors: exposure: 0.50, complexity: 0.50, attack_surface: 0.70
  Description: Adversaries can provide contradictory destinations when sending messages. Traffic is routed in networks using the domain names in various headers available at different levels of the OSI model. In a C...

- Local Execution of Code
  Impact Scores: Financial: 5, Safety: 1, Privacy: 1
  Risk Scores: Financial: 10.649999999999999, Safety: 2.13, Privacy: 2.13
  Risk Factors: exposure: 0.50, complexity: 0.50, attack_surface: 0.70
  Description: An adversary installs and executes malicious code on the target system in an effort to achieve a negative technical impact. Examples include rootkits, ransomware, spyware, adware, and others....

- Object Injection
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5
  Risk Scores: Financial: 2.13, Safety: 2.13, Privacy: 10.649999999999999
  Risk Factors: exposure: 0.50, complexity: 0.50, attack_surface: 0.70
  Description: An adversary attempts to exploit an application by injecting additional, malicious content during its processing of serialized objects. Developers leverage serialization in order to convert data or st...

- Root/Jailbreak Detection Evasion via Debugging
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5
  Risk Scores: Financial: 2.13, Safety: 2.13, Privacy: 10.649999999999999
  Risk Factors: exposure: 0.50, complexity: 0.50, attack_surface: 0.70
  Description: An adversary inserts a debugger into the program entry point of a mobile application to modify the application binary, with the goal of evading Root/Jailbreak detection. Mobile device users often Root...

- Bluetooth Impersonation AttackS (BIAS)
  Impact Scores: Financial: 5, Safety: 1, Privacy: 1
  Risk Scores: Financial: 10.649999999999999, Safety: 2.13, Privacy: 2.13
  Risk Factors: exposure: 0.50, complexity: 0.50, attack_surface: 0.70
  Description: An adversary disguises the MAC address of their Bluetooth enabled device to one for which there exists an active and trusted connection and authenticates successfully. The adversary can then perform m...

- Alteration of a Software Update
  Impact Scores: Financial: 5, Safety: 1, Privacy: 1
  Risk Scores: Financial: 10.649999999999999, Safety: 2.13, Privacy: 2.13
  Risk Factors: exposure: 0.50, complexity: 0.50, attack_surface: 0.70
  Description: An adversary with access to an organization's software update infrastructure inserts malware into the content of an outgoing update to fielded systems where a wide range of malicious effects are possi...

- Exploitation of Improperly Controlled Hardware Security Identifiers
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5
  Risk Scores: Financial: 2.13, Safety: 2.13, Privacy: 10.649999999999999
  Risk Factors: exposure: 0.50, complexity: 0.50, attack_surface: 0.70

Description: An adversary takes advantage of missing or incorrectly configured security identifiers (e.g., tokens), which are used for access control within a System-on-Chip (SoC), to read/write data or execute a ...

- Eavesdropping on a Monitor
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5
  Risk Scores: Financial: 2.13, Safety: 2.13, Privacy: 10.649999999999999
  Risk Factors: exposure: 0.50, complexity: 0.50, attack_surface: 0.70
  Description: An Adversary can eavesdrop on the content of an external monitor through the air without modifying any cable or installing software, just capturing this signal emitted by the cable or video port, with...

- Browser in the Middle (BiTM)
  Impact Scores: Financial: 5, Safety: 1, Privacy: 1
  Risk Scores: Financial: 10.649999999999999, Safety: 2.13, Privacy: 2.13
  Risk Factors: exposure: 0.50, complexity: 0.50, attack_surface: 0.70
  Description: An adversary exploits the inherent functionalities of a web browser, in order to establish an unnoticed remote desktop connection in the victim's browser to the adversary's system. The adversary must ...

- Manipulating State
  Impact Scores: Financial: 1.4, Safety: 1, Privacy: 5
  Risk Scores: Financial: 2.9819999999999998, Safety: 2.13, Privacy: 10.649999999999999
  Risk Factors: exposure: 0.50, complexity: 0.50, attack_surface: 0.70
  Description: The adversary modifies state information maintained by the target software or causes a state transition in hardware. If successful, the target will use this tainted state and execute in an unintended ...

- Interface Manipulation
  Impact Scores: Financial: 4.199999999999999, Safety: 1, Privacy: 1
  Risk Scores: Financial: 8.945999999999998, Safety: 2.13, Privacy: 2.13
  Risk Factors: exposure: 0.50, complexity: 0.50, attack_surface: 0.70
  Description: An adversary manipulates the use or processing of an interface (e.g. Application Programming Interface (API) or System-on-Chip (SoC)) resulting in an adverse impact upon the security of the system imp...

- Parameter Injection
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.199999999999999
  Risk Scores: Financial: 2.13, Safety: 2.13, Privacy: 8.945999999999998
  Risk Factors: exposure: 0.50, complexity: 0.50, attack_surface: 0.70
  Description: An adversary manipulates the content of request parameters for the purpose of undermining the security of the target. Some parameter encodings use text characters as separators. For example, parameter...

- Content Spoofing
  Impact Scores: Financial: 4.199999999999999, Safety: 1, Privacy: 4.199999999999999
  Risk Scores: Financial: 8.945999999999998, Safety: 2.13, Privacy: 8.945999999999998
  Risk Factors: exposure: 0.50, complexity: 0.50, attack_surface: 0.70
  Description: An adversary modifies content to make it contain something other than what the original content producer intended while keeping the apparent source of the content unchanged. The term content spoofing ...

- Resource Location Spoofing
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.199999999999999
  Risk Scores: Financial: 2.13, Safety: 2.13, Privacy: 8.945999999999998
  Risk Factors: exposure: 0.50, complexity: 0.50, attack_surface: 0.70
  Description: An adversary deceives an application or user and convinces them to request a resource from an unintended location. By spoofing the location, the adversary can cause an alternate resource to be used, o...

- Cross-Site Flashing

  Impact Scores: Financial: 4.199999999999999, Safety: 1, Privacy: 1
  Risk Scores: Financial: 8.945999999999998, Safety: 2.13, Privacy: 2.13
  Risk Factors: exposure: 0.50, complexity: 0.50, attack_surface: 0.70
  Description: An attacker is able to trick the victim into executing a Flash document that passes commands or calls to a Flash player browser plugin, allowing the attacker to exploit native Flash functionality in t...

- Modification of Registry Run Keys
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.199999999999999
  Risk Scores: Financial: 2.13, Safety: 2.13, Privacy: 8.945999999999998
  Risk Factors: exposure: 0.50, complexity: 0.50, attack_surface: 0.70
  Description: An adversary adds a new entry to the run keys in the Windows registry so that an application of their choosing is executed when a user logs in. In this way, the adversary can get their executable to o...

- Using Leading 'Ghost' Character Sequences to Bypass Input Filters
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.199999999999999
  Risk Scores: Financial: 2.13, Safety: 2.13, Privacy: 8.945999999999998
  Risk Factors: exposure: 0.50, complexity: 0.50, attack_surface: 0.70
  Description: Some APIs will strip certain leading characters from a string of parameters. An adversary can intentionally introduce leading ghost characters (extra characters that don't affect the validity of the r...

- Manipulate Human Behavior
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.199999999999999
  Risk Scores: Financial: 2.13, Safety: 2.13, Privacy: 8.945999999999998
  Risk Factors: exposure: 0.50, complexity: 0.50, attack_surface: 0.70
  Description: An adversary exploits inherent human psychological predisposition to influence a targeted individual or group to solicit information or manipulate the target into performing an action that serves the ...

- Disable Security Software
  Impact Scores: Financial: 4.199999999999999, Safety: 1, Privacy: 1
  Risk Scores: Financial: 8.945999999999998, Safety: 2.13, Privacy: 2.13
  Risk Factors: exposure: 0.50, complexity: 0.50, attack_surface: 0.70
  Description: An adversary exploits a weakness in access control to disable security tools so that detection does not occur. This can take the form of killing processes, deleting registry keys so that tools do not ...

- Collect Data from Registries
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.199999999999999
  Risk Scores: Financial: 2.13, Safety: 2.13, Privacy: 8.945999999999998
  Risk Factors: exposure: 0.50, complexity: 0.50, attack_surface: 0.70
  Description: An adversary exploits a weakness in authorization to gather system-specific data and sensitive information within a registry (e.g., Windows Registry, Mac plist). These contain information about the sy...

- Collect Data from Screen Capture
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.199999999999999
  Risk Scores: Financial: 2.13, Safety: 2.13, Privacy: 8.945999999999998
  Risk Factors: exposure: 0.50, complexity: 0.50, attack_surface: 0.70
  Description: An adversary gathers sensitive information by exploiting the system's screen capture functionality. Through screenshots, the adversary aims to see what happens on the screen over the course of an oper...

- Retrieve Data from Decommissioned Devices
  Impact Scores: Financial: 1, Safety: 1.4, Privacy: 4.199999999999999
  Risk Scores: Financial: 2.13, Safety: 2.9819999999999998, Privacy: 8.945999999999998
  Risk Factors: exposure: 0.50, complexity: 0.50, attack_surface: 0.70
  Description: An adversary obtains decommissioned, recycled, or discarded systems and devices that can include an

organization’s intellectual property, employee data, and other types of controlled information. Syst...

- Web Application Fingerprinting
  Impact Scores: Financial: 1, Safety: 1, Privacy: 2.8
  Risk Scores: Financial: 2.84, Safety: 2.84, Privacy: 7.951999999999999
  Risk Factors: exposure: 0.50, complexity: 0.50, attack_surface: 0.70
  Description: An attacker sends a series of probes to a web application in order to elicit version-dependent and type-dependent behavior that assists in identifying the target. An attacker could learn information s...

- Fuzzing for application mapping
  Impact Scores: Financial: 1, Safety: 2.8, Privacy: 1
  Risk Scores: Financial: 2.84, Safety: 7.951999999999999, Privacy: 2.84
  Risk Factors: exposure: 0.50, complexity: 0.50, attack_surface: 0.70
  Description: An attacker sends random, malformed, or otherwise unexpected messages to a target application and observes the application's log or error messages returned. The attacker does not initially know how a ...

- AJAX Footprinting
  Impact Scores: Financial: 1, Safety: 1, Privacy: 2.8
  Risk Scores: Financial: 2.84, Safety: 2.84, Privacy: 7.951999999999999
  Risk Factors: exposure: 0.50, complexity: 0.50, attack_surface: 0.70
  Description: This attack utilizes the frequent client-server roundtrips in Ajax conversation to scan a system. While Ajax does not open up new vulnerabilities per se, it does optimize them from an attacker point o...

- ECU Firmware Tampering
  Impact Scores: Financial: 5, Safety: 5, Privacy: 4.199999999999999
  Risk Scores: Financial: 7.1, Safety: 7.1, Privacy: 5.963999999999999
  Risk Factors: exposure: 0.50, complexity: 0.50, attack_surface: 0.70
  Description: Unauthorized modification of ECU firmware causing safety issues...

- Command Line Execution through SQL Injection
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5
  Risk Scores: Financial: 1.42, Safety: 1.42, Privacy: 7.1
  Risk Factors: exposure: 0.50, complexity: 0.50, attack_surface: 0.70
  Description: An attacker uses standard SQL injection methods to inject data into the command line for execution. This could be done directly through misuse of directives such as MSSQL_xp_cmdshell or indirectly thr...

- Escaping a Sandbox by Calling Code in Another Language
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5
  Risk Scores: Financial: 1.42, Safety: 1.42, Privacy: 7.1
  Risk Factors: exposure: 0.50, complexity: 0.50, attack_surface: 0.70
  Description: The attacker may submit malicious code of another language to obtain access to privileges that were not intentionally exposed by the sandbox, thus escaping the sandbox. For instance, Java code cannot ...

- Forced Deadlock
  Impact Scores: Financial: 5, Safety: 1, Privacy: 1
  Risk Scores: Financial: 7.1, Safety: 1.42, Privacy: 1.42
  Risk Factors: exposure: 0.50, complexity: 0.50, attack_surface: 0.70
  Description: The adversary triggers and exploits a deadlock condition in the target software to cause a denial of service. A deadlock can occur when two or more competing actions are waiting for each other to fini...

- Schema Poisoning
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5
  Risk Scores: Financial: 1.42, Safety: 1.42, Privacy: 7.1

  Risk Factors: exposure: 0.50, complexity: 0.50, attack_surface: 0.70
  Description: An adversary corrupts or modifies the content of a schema for the purpose of undermining the security of the target. Schemas provide the structure and content definitions for resources used by an appl...

- Hijacking a Privileged Thread of Execution
  Impact Scores: Financial: 5, Safety: 1, Privacy: 1
  Risk Scores: Financial: 7.1, Safety: 1.42, Privacy: 1.42
  Risk Factors: exposure: 0.50, complexity: 0.50, attack_surface: 0.70
  Description: An adversary hijacks a privileged thread of execution by injecting malicious code into a running process. By using a privleged thread to do their bidding, adversaries can evade process-based detection...

- USB Memory Attacks
  Impact Scores: Financial: 2.8, Safety: 1, Privacy: 5
  Risk Scores: Financial: 3.9759999999999995, Safety: 1.42, Privacy: 7.1
  Risk Factors: exposure: 0.50, complexity: 0.50, attack_surface: 0.70
  Description: An adversary loads malicious code onto a USB memory stick in order to infect any system which the device is plugged in to. USB drives present a significant security risk for business and government ag...

- Signature Spoofing by Misrepresentation
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5
  Risk Scores: Financial: 1.42, Safety: 1.42, Privacy: 7.1
  Risk Factors: exposure: 0.50, complexity: 0.50, attack_surface: 0.70
  Description: An attacker exploits a weakness in the parsing or display code of the recipient software to generate a data blob containing a supposedly valid signature, but the signer's identity is falsely represent...

- Hardware Component Substitution During Baselining
  Impact Scores: Financial: 5, Safety: 1, Privacy: 1
  Risk Scores: Financial: 7.1, Safety: 1.42, Privacy: 1.42
  Risk Factors: exposure: 0.50, complexity: 0.50, attack_surface: 0.70
  Description: An adversary with access to system components during allocated baseline development can substitute a maliciously altered hardware component for a baseline component during the product development and ...

- Malicious Hardware Update
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5
  Risk Scores: Financial: 1.42, Safety: 1.42, Privacy: 7.1
  Risk Factors: exposure: 0.50, complexity: 0.50, attack_surface: 0.70
  Description: An adversary introduces malicious hardware during an update or replacement procedure, allowing for additional compromise or site disruption at the victim location. After deployment, it is not uncommon...

- Open-Source Library Manipulation
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5
  Risk Scores: Financial: 1.42, Safety: 1.42, Privacy: 7.1
  Risk Factors: exposure: 0.50, complexity: 0.50, attack_surface: 0.70
  Description: Adversaries implant malicious code in open source software (OSS) libraries to have it widely distributed, as OSS is commonly downloaded by developers and other users to incorporate into software devel...

- ASIC With Malicious Functionality
  Impact Scores: Financial: 5, Safety: 1, Privacy: 1
  Risk Scores: Financial: 7.1, Safety: 1.42, Privacy: 1.42
  Risk Factors: exposure: 0.50, complexity: 0.50, attack_surface: 0.70
  Description: An attacker with access to the development environment process of an application-specific integrated circuit (ASIC) for a victim system being developed or maintained after initial deployment can inser...

- Replace Trusted Executable
  Impact Scores: Financial: 5, Safety: 1, Privacy: 1
  Risk Scores: Financial: 7.1, Safety: 1.42, Privacy: 1.42
  Risk Factors: exposure: 0.50, complexity: 0.50, attack_surface: 0.70
  Description: An adversary exploits weaknesses in privilege management or access control to replace a trusted executable with a malicious version and enable the execution of malware when that trusted executable is ...

- Hardware Fault Injection
  Impact Scores: Financial: 1, Safety: 5, Privacy: 5
  Risk Scores: Financial: 1.42, Safety: 7.1, Privacy: 7.1
  Risk Factors: exposure: 0.50, complexity: 0.50, attack_surface: 0.70
  Description: The adversary uses disruptive signals or events, or alters the physical environment a device operates in, to cause faulty behavior in electronic devices. This can include electromagnetic pulses, laser...

- Carry-Off GPS Attack
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5
  Risk Scores: Financial: 1.42, Safety: 1.42, Privacy: 7.1
  Risk Factors: exposure: 0.50, complexity: 0.50, attack_surface: 0.70
  Description: A common form of a GPS spoofing attack, commonly termed a carry-off attack begins with an adversary broadcasting signals synchronized with the genuine signals observed by the target receiver. The powe...

- DLL Side-Loading
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5
  Risk Scores: Financial: 1.42, Safety: 1.42, Privacy: 7.1
  Risk Factors: exposure: 0.50, complexity: 0.50, attack_surface: 0.70
  Description: An adversary places a malicious version of a Dynamic-Link Library (DLL) in the Windows Side-by-Side (WinSxS) directory to trick the operating system into loading this malicious DLL instead of a legiti...

- Use of Captured Tickets (Pass The Ticket)
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5
  Risk Scores: Financial: 1.42, Safety: 1.42, Privacy: 7.1
  Risk Factors: exposure: 0.50, complexity: 0.50, attack_surface: 0.70
  Description: An adversary uses stolen Kerberos tickets to access systems/resources that leverage the Kerberos authentication protocol. The Kerberos authentication protocol centers around a ticketing system which i...

- Sniff Application Code
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5
  Risk Scores: Financial: 1.42, Safety: 1.42, Privacy: 7.1
  Risk Factors: exposure: 0.50, complexity: 0.50, attack_surface: 0.70
  Description: An adversary passively sniffs network communications and captures application code bound for an authorized client. Once obtained, they can use it as-is, or through reverse-engineering glean sensitive ...

- Exploitation of Transient Instruction Execution
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5
  Risk Scores: Financial: 1.42, Safety: 1.42, Privacy: 7.1
  Risk Factors: exposure: 0.50, complexity: 0.50, attack_surface: 0.70
  Description: An adversary exploits a hardware design flaw in a CPU implementation of transient instruction execution to expose sensitive data and bypass/subvert access control over restricted resources. Typically,...

- Key Negotiation of Bluetooth Attack (KNOB)
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5
  Risk Scores: Financial: 1.42, Safety: 1.42, Privacy: 7.1
  Risk Factors: exposure: 0.50, complexity: 0.50, attack_surface: 0.70

Description: An adversary can exploit a flaw in Bluetooth key negotiation allowing them to decrypt information sent between two devices communicating via Bluetooth. The adversary uses an Adversary in the Middle se...

- Malicious Code Implanted During Chip Programming
  Impact Scores: Financial: 5, Safety: 1, Privacy: 1
  Risk Scores: Financial: 7.1, Safety: 1.42, Privacy: 1.42
  Risk Factors: exposure: 0.50, complexity: 0.50, attack_surface: 0.70
  Description: During the programming step of chip manufacture, an adversary with access and necessary technical skills maliciously alters a chip’s intended program logic to produce an effect intended by the adversa...

- Subvert Code-signing Facilities
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5
  Risk Scores: Financial: 1.42, Safety: 1.42, Privacy: 7.1
  Risk Factors: exposure: 0.50, complexity: 0.50, attack_surface: 0.70
  Description: Many languages use code signing facilities to vouch for code's identity and to thus tie code to its assigned privileges within an environment. Subverting this mechanism can be instrumental in an attac...

- Load Value Injection
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5
  Risk Scores: Financial: 1.42, Safety: 1.42, Privacy: 7.1
  Risk Factors: exposure: 0.50, complexity: 0.50, attack_surface: 0.70
  Description: An adversary exploits a hardware design flaw in a CPU implementation of transient instruction execution in which a faulting or assisted load instruction transiently forwards adversary-controlled data ...

- Active OS Fingerprinting
  Impact Scores: Financial: 1, Safety: 1, Privacy: 2.8
  Risk Scores: Financial: 2.13, Safety: 2.13, Privacy: 5.9639999999999995
  Risk Factors: exposure: 0.50, complexity: 0.50, attack_surface: 0.70
  Description: An adversary engages in activity to detect the operating system or firmware version of a remote target by interrogating a device, server, or platform with a probe designed to solicit behavior that wil...

- TCP Timestamp Probe
  Impact Scores: Financial: 2.8, Safety: 1, Privacy: 1
  Risk Scores: Financial: 5.9639999999999995, Safety: 2.13, Privacy: 2.13
  Risk Factors: exposure: 0.50, complexity: 0.50, attack_surface: 0.70
  Description: This OS fingerprinting probe examines the remote server's implementation of TCP timestamps. Not all operating systems implement timestamps within the TCP header, but when timestamps are used then this...

- TCP Sequence Number Probe
  Impact Scores: Financial: 2.8, Safety: 1, Privacy: 1
  Risk Scores: Financial: 5.9639999999999995, Safety: 2.13, Privacy: 2.13
  Risk Factors: exposure: 0.50, complexity: 0.50, attack_surface: 0.70
  Description: This OS fingerprinting probe tests the target system's assignment of TCP sequence numbers. One common way to test TCP Sequence Number generation is to send a probe packet to an open port on the target...

- TCP (ISN) Greatest Common Divisor Probe
  Impact Scores: Financial: 1, Safety: 1, Privacy: 2.8
  Risk Scores: Financial: 2.13, Safety: 2.13, Privacy: 5.9639999999999995
  Risk Factors: exposure: 0.50, complexity: 0.50, attack_surface: 0.70
  Description: This OS fingerprinting probe sends a number of TCP SYN packets to an open port of a remote machine. The Initial Sequence Number (ISN) in each of the SYN/ACK response packets is analyzed to determine t...

- TCP (ISN) Counter Rate Probe

Impact Scores: Financial: 1, Safety: 1, Privacy: 2.8
Risk Scores: Financial: 2.13, Safety: 2.13, Privacy: 5.9639999999999995
Risk Factors: exposure: 0.50, complexity: 0.50, attack_surface: 0.70
Description: This OS detection probe measures the average rate of initial sequence number increments during a period of time. Sequence numbers are incremented using a time-based algorithm and are susceptible to a ...

- TCP (ISN) Sequence Predictability Probe
  Impact Scores: Financial: 1, Safety: 1, Privacy: 2.8
  Risk Scores: Financial: 2.13, Safety: 2.13, Privacy: 5.9639999999999995
  Risk Factors: exposure: 0.50, complexity: 0.50, attack_surface: 0.70
  Description: This type of operating system probe attempts to determine an estimate for how predictable the sequence number generation algorithm is for a remote host. Statistical techniques, such as standard deviat...

- TCP Initial Window Size Probe
  Impact Scores: Financial: 2.8, Safety: 1, Privacy: 1
  Risk Scores: Financial: 5.9639999999999995, Safety: 2.13, Privacy: 2.13
  Risk Factors: exposure: 0.50, complexity: 0.50, attack_surface: 0.70
  Description: This OS fingerprinting probe checks the initial TCP Window size. TCP stacks limit the range of sequence numbers allowable within a session to maintain the connected state within TCP protocol logic. Th...

- TCP Options Probe
  Impact Scores: Financial: 2.8, Safety: 1, Privacy: 1
  Risk Scores: Financial: 5.9639999999999995, Safety: 2.13, Privacy: 2.13
  Risk Factors: exposure: 0.50, complexity: 0.50, attack_surface: 0.70
  Description: This OS fingerprinting probe analyzes the type and order of any TCP header options present within a response segment. Most operating systems use unique ordering and different option sets when options ...

- Pretexting
  Impact Scores: Financial: 1, Safety: 1, Privacy: 2.8
  Risk Scores: Financial: 2.13, Safety: 2.13, Privacy: 5.9639999999999995
  Risk Factors: exposure: 0.50, complexity: 0.50, attack_surface: 0.70
  Description: An adversary engages in pretexting behavior to solicit information from target persons, or manipulate the target into performing some action that serves the adversary's interests. During a pretexting ...

- Interception
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.199999999999999
  Risk Scores: Financial: 1.42, Safety: 1.42, Privacy: 5.963999999999999
  Risk Factors: exposure: 0.50, complexity: 0.50, attack_surface: 0.70
  Description: An adversary monitors data streams to or from the target for information gathering purposes. This attack may be undertaken to solely gather sensitive information or to support a further attack against...

- XML Ping of the Death
  Impact Scores: Financial: 1, Safety: 4.199999999999999, Privacy: 1
  Risk Scores: Financial: 1.42, Safety: 5.963999999999999, Privacy: 1.42
  Risk Factors: exposure: 0.50, complexity: 0.50, attack_surface: 0.70
  Description: An attacker initiates a resource depletion attack where a large number of small XML messages are delivered at a sufficiently rapid rate to cause a denial of service or crash of the target. Transaction...

- Incomplete Data Deletion in a Multi-Tenant Environment
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.199999999999999
  Risk Scores: Financial: 1.42, Safety: 1.42, Privacy: 5.963999999999999
  Risk Factors: exposure: 0.50, complexity: 0.50, attack_surface: 0.70
  Description: An adversary obtains unauthorized information due to insecure or incomplete data deletion in a

multi-tenant environment. If a cloud provider fails to completely delete storage and data from former clo...

- Adding a Space to a File Extension
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.199999999999999
  Risk Scores: Financial: 1.42, Safety: 1.42, Privacy: 5.963999999999999
  Risk Factors: exposure: 0.50, complexity: 0.50, attack_surface: 0.70
  Description: An adversary adds a space character to the end of a file extension and takes advantage of an application that does not properly neutralize trailing special elements in file names. This extra space, wh...

- Reverse Engineering
  Impact Scores: Financial: 2.8, Safety: 1, Privacy: 1
  Risk Scores: Financial: 3.9759999999999995, Safety: 1.42, Privacy: 1.42
  Risk Factors: exposure: 0.50, complexity: 0.50, attack_surface: 0.70
  Description: An adversary discovers the structure, function, and composition of an object, resource, or system by using a variety of analysis techniques to effectively determine how the analyzed entity was constru...

- Fingerprinting
  Impact Scores: Financial: 1, Safety: 1, Privacy: 1.4
  Risk Scores: Financial: 2.84, Safety: 2.84, Privacy: 3.9759999999999995
  Risk Factors: exposure: 0.50, complexity: 0.50, attack_surface: 0.70
  Description: An adversary compares output from a target system to known indicators that uniquely identify specific details about the target. Most commonly, fingerprinting is done to determine operating system and ...

- Target Influence via Framing
  Impact Scores: Financial: 1, Safety: 1.4, Privacy: 2.8
  Risk Scores: Financial: 1.42, Safety: 1.9879999999999998, Privacy: 3.9759999999999995
  Risk Factors: exposure: 0.50, complexity: 0.50, attack_surface: 0.70
  Description: An adversary uses framing techniques to contextualize a conversation so that the target is more likely to be influenced by the adversary's point of view. Framing is information and experiences in life...

- Influence via Psychological Principles
  Impact Scores: Financial: 2.8, Safety: 1, Privacy: 1
  Risk Scores: Financial: 3.9759999999999995, Safety: 1.42, Privacy: 1.42
  Risk Factors: exposure: 0.50, complexity: 0.50, attack_surface: 0.70
  Description: The adversary shapes the target's actions or behavior by focusing on the ways human interact and learn, leveraging such elements as cognitive and social psychology. In a variety of ways, a target can ...

- Process Footprinting
  Impact Scores: Financial: 1, Safety: 1, Privacy: 2.8
  Risk Scores: Financial: 1.42, Safety: 1.42, Privacy: 3.9759999999999995
  Risk Factors: exposure: 0.50, complexity: 0.50, attack_surface: 0.70
  Description: An adversary exploits functionality meant to identify information about the currently running processes on the target system to an authorized user. By knowing what processes are running on the target ...

- Services Footprinting
  Impact Scores: Financial: 1, Safety: 1, Privacy: 2.8
  Risk Scores: Financial: 1.42, Safety: 1.42, Privacy: 3.9759999999999995
  Risk Factors: exposure: 0.50, complexity: 0.50, attack_surface: 0.70
  Description: An adversary exploits functionality meant to identify information about the services on the target system to an authorized user. By knowing what services are registered on the target system, the adver...

- Account Footprinting
  Impact Scores: Financial: 1, Safety: 1, Privacy: 2.8

Risk Scores: Financial: 1.42, Safety: 1.42, Privacy: 3.9759999999999995
Risk Factors: exposure: 0.50, complexity: 0.50, attack_surface: 0.70
Description: An adversary exploits functionality meant to identify information about the domain accounts and their permissions on the target system to an authorized user. By knowing what accounts are registered on...

- Group Permission Footprinting
  Impact Scores: Financial: 1, Safety: 1, Privacy: 2.8
  Risk Scores: Financial: 1.42, Safety: 1.42, Privacy: 3.9759999999999995
  Risk Factors: exposure: 0.50, complexity: 0.50, attack_surface: 0.70
  Description: An adversary exploits functionality meant to identify information about user groups and their permissions on the target system to an authorized user. By knowing what users/permissions are registered o...

- Owner Footprinting
  Impact Scores: Financial: 1, Safety: 1, Privacy: 2.8
  Risk Scores: Financial: 1.42, Safety: 1.42, Privacy: 3.9759999999999995
  Risk Factors: exposure: 0.50, complexity: 0.50, attack_surface: 0.70
  Description: An adversary exploits functionality meant to identify information about the primary users on the target system to an authorized user. They may do this, for example, by reviewing logins or file modific...

- System Footprinting
  Impact Scores: Financial: 1, Safety: 1, Privacy: 2.8
  Risk Scores: Financial: 1.42, Safety: 1.42, Privacy: 3.9759999999999995
  Risk Factors: exposure: 0.50, complexity: 0.50, attack_surface: 0.70
  Description: An adversary engages in active probing and exploration activities to determine security information about a remote target system. Often times adversaries will rely on remote applications that can be p...

- Collect Data from Clipboard
  Impact Scores: Financial: 1, Safety: 1, Privacy: 2.8
  Risk Scores: Financial: 1.42, Safety: 1.42, Privacy: 3.9759999999999995
  Risk Factors: exposure: 0.50, complexity: 0.50, attack_surface: 0.70
  Description: The adversary exploits an application that allows for the copying of sensitive data or information by collecting information copied to the clipboard. Data copied to the clipboard can be accessed by ot...

Component: Engine Speed Sensor

Type: Sensor
Safety Level: ASIL B
Interfaces: CAN
Access Points:
Data Types: Sensor Data
Location: External
Trust Zone: Untrusted
Connected To: ECU001

Identified Threats:

- Buffer Manipulation
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5
  Risk Scores: Financial: 3.04, Safety: 3.04, Privacy: 15.2
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: An adversary manipulates an application's interaction with a buffer in an attempt to read or modify data

they shouldn't have access to. Buffer attacks are distinguished in that it is the buffer space ...

- Redirect Access to Libraries
  Impact Scores: Financial: 1, Safety: 5, Privacy: 1
  Risk Scores: Financial: 3.04, Safety: 15.2, Privacy: 3.04
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: An adversary exploits a weakness in the way an application searches for external libraries to manipulate the execution flow to point to an adversary supplied library or code base. This pattern of atta...

- XSS Targeting Non-Script Elements
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5
  Risk Scores: Financial: 3.04, Safety: 3.04, Privacy: 15.2
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: This attack is a form of Cross-Site Scripting (XSS) where malicious scripts are embedded in elements that are not expected to host scripts such as image tags (<img>), comments in XML documents (< !-CD...

- Retrieve Embedded Sensitive Data
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5
  Risk Scores: Financial: 3.04, Safety: 3.04, Privacy: 15.2
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: An attacker examines a target system to find sensitive data that has been embedded within it. This information can reveal confidential contents, such as account numbers or individual keys/credentials ...

- Leveraging/Manipulating Configuration File Search Paths
  Impact Scores: Financial: 5, Safety: 1, Privacy: 1
  Risk Scores: Financial: 15.2, Safety: 3.04, Privacy: 3.04
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: This pattern of attack sees an adversary load a malicious resource into a program's standard path so that when a known command is executed then the system instead executes the malicious component. The...

- Manipulating Writeable Terminal Devices
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5
  Risk Scores: Financial: 3.04, Safety: 3.04, Privacy: 15.2
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: This attack exploits terminal devices that allow themselves to be written to by other users. The attacker sends command strings to the target terminal device hoping that the target user will hit enter...

- Overflow Binary Resource File
  Impact Scores: Financial: 5, Safety: 1, Privacy: 1
  Risk Scores: Financial: 15.2, Safety: 3.04, Privacy: 3.04
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: An attack of this type exploits a buffer overflow vulnerability in the handling of binary resources. Binary resources may include music files like MP3, image files like JPEG files, and any other binar...

- Poison Web Service Registry
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5
  Risk Scores: Financial: 3.04, Safety: 3.04, Privacy: 15.2
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: SOA and Web Services often use a registry to perform look up, get schema information, and metadata about services. A poisoned registry can redirect (think phishing for servers) the service requester t...

- String Format Overflow in syslog()
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5

Risk Scores: Financial: 3.04, Safety: 3.04, Privacy: 15.2
Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
Description: This attack targets applications and software that uses the syslog() function insecurely. If an application does not explicitely use a format string parameter in a call to syslog(), user input can be ...

- Manipulating User-Controlled Variables
  Impact Scores: Financial: 2.0, Safety: 1, Privacy: 5
  Risk Scores: Financial: 6.08, Safety: 3.04, Privacy: 15.2
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: This attack targets user controlled variables (DEBUG=1, PHP Globals, and So Forth). An adversary can override variables leveraging user-supplied, untrusted query variables directly used on the applica...

- XQuery Injection
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5
  Risk Scores: Financial: 3.04, Safety: 3.04, Privacy: 15.2
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: This attack utilizes XQuery to probe and attack server systems; in a similar manner that SQL Injection allows an attacker to exploit SQL calls to RDBMS, XQuery Injection uses improperly validated data...

- Pharming
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5
  Risk Scores: Financial: 3.04, Safety: 3.04, Privacy: 15.2
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: A pharming attack occurs when the victim is fooled into entering sensitive data into supposedly trusted locations, such as an online bank site or a trading platform. An attacker can impersonate these ...

- Phishing
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5
  Risk Scores: Financial: 3.04, Safety: 3.04, Privacy: 15.2
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: Phishing is a social engineering technique where an attacker masquerades as a legitimate entity with which the victim might do business in order to prompt the user to reveal some confidential informat...

- Accessing Functionality Not Properly Constrained by ACLs
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.0
  Risk Scores: Financial: 3.04, Safety: 3.04, Privacy: 12.16
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: In applications, particularly web applications, access to functionality is mitigated by an authorization framework. This framework maps Access Control Lists (ACLs) to elements of the application's fun...

- Buffer Overflow via Environment Variables
  Impact Scores: Financial: 4.0, Safety: 1, Privacy: 1
  Risk Scores: Financial: 12.16, Safety: 3.04, Privacy: 3.04
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: This attack pattern involves causing a buffer overflow through manipulation of environment variables. Once the adversary finds that they can modify an environment variable, they may try to overflow as...

- Server Side Include (SSI) Injection
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.0
  Risk Scores: Financial: 3.04, Safety: 3.04, Privacy: 12.16
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: An attacker can use Server Side Include (SSI) Injection to send code to a web application that then gets executed by the web server. Doing so enables the attacker to achieve similar results to Cross S...

- Format String Injection
  Impact Scores: Financial: 1, Safety: 2.0, Privacy: 4.0
  Risk Scores: Financial: 3.04, Safety: 6.08, Privacy: 12.16
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: An adversary includes formatting characters in a string input field on the target application. Most applications assume that users will provide static text and may respond unpredictably to the presenc...

- Cache Poisoning
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.0
  Risk Scores: Financial: 3.04, Safety: 3.04, Privacy: 12.16
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: An attacker exploits the functionality of cache technologies to cause specific data to be cached that aids the attackers' objectives. This describes any attack whereby an attacker places incorrect or ...

- DNS Cache Poisoning
  Impact Scores: Financial: 4.0, Safety: 1, Privacy: 1
  Risk Scores: Financial: 12.16, Safety: 3.04, Privacy: 3.04
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: A domain name server translates a domain name (such as www.example.com) into an IP address that Internet hosts use to contact Internet resources. An adversary modifies a public DNS cache to cause cert...

- Command Delimiters
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.0
  Risk Scores: Financial: 3.04, Safety: 3.04, Privacy: 12.16
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: An attack of this type exploits a programs' vulnerabilities that allows an attacker's commands to be concatenated onto a legitimate command with the intent of targeting other resources such as the fil...

- Malicious Automated Software Update via Redirection
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.0
  Risk Scores: Financial: 3.04, Safety: 3.04, Privacy: 12.16
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: An attacker exploits two layers of weaknesses in server or client software for automated update mechanisms to undermine the integrity of the target code-base. The first weakness involves a failure to ...

- PHP Remote File Inclusion
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.0
  Risk Scores: Financial: 3.04, Safety: 3.04, Privacy: 12.16
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: In this pattern the adversary is able to load and execute arbitrary code remotely available from the application. This is usually accomplished through an insecurely configured PHP runtime environment ...

- XSS Using Alternate Syntax
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.0
  Risk Scores: Financial: 3.04, Safety: 3.04, Privacy: 12.16
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: An adversary uses alternate forms of keywords or commands that result in the same action as the primary form but which may not be caught by filters. For example, many keywords are processed in a case ...

- Serialized Data External Linking
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.0
  Risk Scores: Financial: 3.04, Safety: 3.04, Privacy: 12.16
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20

Description: An adversary creates a serialized data file (e.g. XML, YAML, etc...) that contains an external data reference. Because serialized data parsers may not validate documents with external references, ther...

- Leveraging Race Conditions
  Impact Scores: Financial: 4.0, Safety: 1, Privacy: 1
  Risk Scores: Financial: 12.16, Safety: 3.04, Privacy: 3.04
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: The adversary targets a race condition occurring when multiple processes access and manipulate the same resource concurrently, and the outcome of the execution depends on the particular order in which...

- Leveraging Time-of-Check and Time-of-Use (TOCTOU) Race Conditions
  Impact Scores: Financial: 4.0, Safety: 1, Privacy: 1
  Risk Scores: Financial: 12.16, Safety: 3.04, Privacy: 3.04
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: This attack targets a race condition occurring between the time of check (state) for a resource and the time of use of a resource. A typical example is file access. The adversary can leverage a file a...

- Using Meta-characters in E-mail Headers to Inject Malicious Payloads
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.0
  Risk Scores: Financial: 3.04, Safety: 3.04, Privacy: 12.16
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: This type of attack involves an attacker leveraging meta-characters in email headers to inject improper behavior into email programs. Email software has become increasingly sophisticated and feature-r...

- Buffer Overflow via Symbolic Links
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.0
  Risk Scores: Financial: 3.04, Safety: 3.04, Privacy: 12.16
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: This type of attack leverages the use of symbolic links to cause buffer overflows. An adversary can try to create or manipulate a symbolic link file such that its contents result in out of bounds data...

- Passing Local Filenames to Functions That Expect a URL
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.0
  Risk Scores: Financial: 3.04, Safety: 3.04, Privacy: 12.16
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: This attack relies on client side code to access local files and resources instead of URLs. When the client browser is expecting a URL string, but instead receives a request for a local file, that exe...

- Session Credential Falsification through Prediction
  Impact Scores: Financial: 4.0, Safety: 1, Privacy: 1
  Risk Scores: Financial: 12.16, Safety: 3.04, Privacy: 3.04
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: This attack targets predictable session ID in order to gain privileges. The attacker can predict the session ID used during a transaction to perform spoofing and session hijacking....

- Using Slashes and URL Encoding Combined to Bypass Validation Logic
  Impact Scores: Financial: 4.0, Safety: 1, Privacy: 1
  Risk Scores: Financial: 12.16, Safety: 3.04, Privacy: 3.04
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: This attack targets the encoding of the URL combined with the encoding of the slash characters. An attacker can take advantage of the multiple ways of encoding a URL and abuse the interpretation of th...

- Voice Phishing

Impact Scores: Financial: 1, Safety: 1, Privacy: 4.0
Risk Scores: Financial: 3.04, Safety: 3.04, Privacy: 12.16
Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
Description: An adversary targets users with a phishing attack for the purpose of soliciting account passwords or sensitive information from the user. Voice Phishing is a variation of the Phishing social engineeri...

- Malicious Automated Software Update via Spoofing
Impact Scores: Financial: 1, Safety: 1, Privacy: 4.0
Risk Scores: Financial: 3.04, Safety: 3.04, Privacy: 12.16
Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
Description: An attackers uses identify or content spoofing to trick a client into performing an automated software update from a malicious source. A malicious automated software update that leverages spoofing can...

- Blind SQL Injection
Impact Scores: Financial: 1, Safety: 1, Privacy: 4.0
Risk Scores: Financial: 3.04, Safety: 3.04, Privacy: 12.16
Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
Description: Blind SQL Injection results from an insufficient mitigation for SQL Injection. Although suppressing database error messages are considered best practice, the suppression alone is not sufficient to pre...

- URL Encoding
Impact Scores: Financial: 4.0, Safety: 1, Privacy: 1
Risk Scores: Financial: 12.16, Safety: 3.04, Privacy: 3.04
Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
Description: This attack targets the encoding of the URL. An adversary can take advantage of the multiple way of encoding an URL and abuse the interpretation of the URL....

- User-Controlled Filename
Impact Scores: Financial: 1, Safety: 1, Privacy: 4.0
Risk Scores: Financial: 3.04, Safety: 3.04, Privacy: 12.16
Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
Description: An attack of this type involves an adversary inserting malicious characters (such as a XSS redirection) into a filename, directly or indirectly that is then used by the target software to generate HTM...

- Using Escaped Slashes in Alternate Encoding
Impact Scores: Financial: 4.0, Safety: 1, Privacy: 1
Risk Scores: Financial: 12.16, Safety: 3.04, Privacy: 3.04
Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
Description: This attack targets the use of the backslash in alternate encoding. An adversary can provide a backslash as a leading character and causes a parser to believe that the next character is special. This ...

- Buffer Overflow in an API Call
Impact Scores: Financial: 4.0, Safety: 1, Privacy: 1
Risk Scores: Financial: 12.16, Safety: 3.04, Privacy: 3.04
Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
Description: This attack targets libraries or shared code modules which are vulnerable to buffer overflow attacks. An adversary who has knowledge of known vulnerable libraries or shared code can easily target soft...

- Using UTF-8 Encoding to Bypass Validation Logic
Impact Scores: Financial: 1, Safety: 4.0, Privacy: 1
Risk Scores: Financial: 3.04, Safety: 12.16, Privacy: 3.04
Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
Description: This attack is a specific variation on leveraging alternate encodings to bypass validation logic. This attack

leverages the possibility to encode potentially harmful input in UTF-8 and submit it to ap...

- XPath Injection
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.0
  Risk Scores: Financial: 3.04, Safety: 3.04, Privacy: 12.16
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: An attacker can craft special user-controllable input consisting of XPath expressions to inject the XML database and bypass authentication or glean information that they normally would not be able to....

- OS Command Injection
  Impact Scores: Financial: 4.0, Safety: 1, Privacy: 1
  Risk Scores: Financial: 12.16, Safety: 3.04, Privacy: 3.04
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: In this type of an attack, an adversary injects operating system commands into existing application functions. An application that uses untrusted input to build command strings is vulnerable. An adver...

- Buffer Overflow in Local Command-Line Utilities
  Impact Scores: Financial: 4.0, Safety: 1, Privacy: 1
  Risk Scores: Financial: 12.16, Safety: 3.04, Privacy: 3.04
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: This attack targets command-line utilities available in a number of shells. An adversary can leverage a vulnerability found in a command-line utility to escalate privilege to root....

- Reflection Attack in Authentication Protocol
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.0
  Risk Scores: Financial: 3.04, Safety: 3.04, Privacy: 12.16
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: An adversary can abuse an authentication protocol susceptible to reflection attack in order to defeat it. Doing so allows the adversary illegitimate access to the target system, without possessing the...

- Forced Integer Overflow
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.0
  Risk Scores: Financial: 3.04, Safety: 3.04, Privacy: 12.16
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: This attack forces an integer variable to go out of range. The integer variable is often used as an offset such as size of memory allocation or similarly. The attacker would typically control the valu...

- WSDL Scanning
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.0
  Risk Scores: Financial: 3.04, Safety: 3.04, Privacy: 12.16
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: This attack targets the WSDL interface made available by a web service. The attacker may scan the WSDL interface to reveal sensitive information about invocation patterns, underlying technology implem...

- Root/Jailbreak Detection Evasion via Debugging
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5
  Risk Scores: Financial: 2.2800000000000002, Safety: 2.2800000000000002, Privacy: 11.400000000000002
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: An adversary inserts a debugger into the program entry point of a mobile application to modify the application binary, with the goal of evading Root/Jailbreak detection. Mobile device users often Root...

- CAN Injection
  Impact Scores: Financial: 3.0, Safety: 4.0, Privacy: 2.0

```
  Risk Scores: Financial: 6.840000000000001, Safety: 9.120000000000001, Privacy: 4.5600000000000005
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: Manipulation of CAN bus messages leading to vehicle malfunction...

- Sensor Data Manipulation
  Impact Scores: Financial: 3.0, Safety: 4.0, Privacy: 2.0
  Risk Scores: Financial: 6.840000000000001, Safety: 9.120000000000001, Privacy: 4.5600000000000005
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: Tampering with sensor data leading to incorrect vehicle behavior...

- HTTP Request Splitting
  Impact Scores: Financial: 4.0, Safety: 1, Privacy: 1
  Risk Scores: Financial: 9.120000000000001, Safety: 2.2800000000000002, Privacy: 2.2800000000000002
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: An adversary abuses the flexibility and discrepancies in the parsing and interpretation of HTTP Request messages by different intermediary HTTP agents (e.g., load balancer, reverse proxy, web caching ...

- Flooding
  Impact Scores: Financial: 1, Safety: 1, Privacy: 3.0
  Risk Scores: Financial: 3.04, Safety: 3.04, Privacy: 9.120000000000001
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: An adversary consumes the resources of a target by rapidly engaging in a large number of interactions with the target. This type of attack generally exposes a weakness in rate limiting or flow. When s...

- Directory Indexing
  Impact Scores: Financial: 1, Safety: 1, Privacy: 3.0
  Risk Scores: Financial: 3.04, Safety: 3.04, Privacy: 9.120000000000001
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: An adversary crafts a request to a target that results in the target listing/indexing the content of a directory as output. One common method of triggering directory contents as output is to construct...

- Flash Parameter Injection
  Impact Scores: Financial: 1, Safety: 1, Privacy: 3.0
  Risk Scores: Financial: 3.04, Safety: 3.04, Privacy: 9.120000000000001
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: An adversary takes advantage of improper data validation to inject malicious global parameters into a Flash file embedded within an HTML document. Flash files can leverage user-submitted data to confi...

- Exploiting Incorrectly Configured Access Control Security Levels
  Impact Scores: Financial: 1, Safety: 1, Privacy: 3.0
  Risk Scores: Financial: 3.04, Safety: 3.04, Privacy: 9.120000000000001
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: An attacker exploits a weakness in the configuration of access controls and is able to bypass the intended protection that these measures guard against and thereby obtain unauthorized access to the sy...

- Exponential Data Expansion
  Impact Scores: Financial: 1, Safety: 1, Privacy: 3.0
  Risk Scores: Financial: 3.04, Safety: 3.04, Privacy: 9.120000000000001
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: An adversary submits data to a target application which contains nested exponential data expansion to produce excessively large output. Many data format languages allow the definition of macro-like st...

- Inducing Account Lockout
```

Impact Scores: Financial: 1, Safety: 1, Privacy: 3.0
Risk Scores: Financial: 3.04, Safety: 3.04, Privacy: 9.120000000000001
Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
Description: An attacker leverages the security functionality of the system aimed at thwarting potential attacks to launch a denial of service attack against a legitimate system user. Many systems, for instance, i...

- XML Routing Detour Attacks
  Impact Scores: Financial: 1, Safety: 1, Privacy: 3.0
  Risk Scores: Financial: 3.04, Safety: 3.04, Privacy: 9.120000000000001
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: An attacker subverts an intermediate system used to process XML content and forces the intermediate to modify and/or re-route the processing of the content. XML Routing Detour Attacks are Adversary in...

- Serialized Data with Nested Payloads
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.0
  Risk Scores: Financial: 2.2800000000000002, Safety: 2.2800000000000002, Privacy: 9.120000000000001
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: Applications often need to transform data in and out of a data format (e.g., XML and YAML) by using a parser. It may be possible for an adversary to inject data that may have an adverse effect on the ...

- Command Injection
  Impact Scores: Financial: 4.0, Safety: 1, Privacy: 1
  Risk Scores: Financial: 9.120000000000001, Safety: 2.2800000000000002, Privacy: 2.2800000000000002
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: An adversary looking to execute a command of their choosing, injects new items into an existing command thus modifying interpretation away from what was intended. Commands in this context are often st...

- Leveraging Race Conditions via Symbolic Links
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.0
  Risk Scores: Financial: 2.2800000000000002, Safety: 2.2800000000000002, Privacy: 9.120000000000001
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: This attack leverages the use of symbolic links (Symlinks) in order to write to sensitive files. An attacker can create a Symlink link to a target file not otherwise accessible to them. When the privi...

- HTTP Response Smuggling
  Impact Scores: Financial: 4.0, Safety: 1, Privacy: 1
  Risk Scores: Financial: 9.120000000000001, Safety: 2.2800000000000002, Privacy: 2.2800000000000002
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: An adversary manipulates and injects malicious content in the form of secret unauthorized HTTP responses, into a single HTTP response from a vulnerable or compromised back-end HTTP agent (e.g., server...

- SOAP Manipulation
  Impact Scores: Financial: 4.0, Safety: 1, Privacy: 1
  Risk Scores: Financial: 9.120000000000001, Safety: 2.2800000000000002, Privacy: 2.2800000000000002
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: Simple Object Access Protocol (SOAP) is used as a communication protocol between a client and server to invoke web services on the server. It is an XML-based protocol, and therefore suffers from many ...

- Fuzzing
  Impact Scores: Financial: 1, Safety: 1, Privacy: 3.0
  Risk Scores: Financial: 3.04, Safety: 3.04, Privacy: 9.120000000000001
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: In this attack pattern, the adversary leverages fuzzing to try to identify weaknesses in the system. Fuzzing

is a software security and functionality testing method that feeds randomly constructed inp...

- HTTP Request Smuggling
  Impact Scores: Financial: 4.0, Safety: 1, Privacy: 1
  Risk Scores: Financial: 9.120000000000001, Safety: 2.2800000000000002, Privacy: 2.2800000000000002
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: An adversary abuses the flexibility and discrepancies in the parsing and interpretation of HTTP Request messages using various HTTP headers, request-line and body parameters as well as message sizes (...

- HTTP Response Splitting
  Impact Scores: Financial: 4.0, Safety: 1, Privacy: 1
  Risk Scores: Financial: 9.120000000000001, Safety: 2.2800000000000002, Privacy: 2.2800000000000002
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: An adversary manipulates and injects malicious content, in the form of secret unauthorized HTTP responses, into a single HTTP response from a vulnerable or compromised back-end HTTP agent (e.g., web s...

- Manipulating Opaque Client-based Data Tokens
  Impact Scores: Financial: 1, Safety: 1, Privacy: 3.0
  Risk Scores: Financial: 3.04, Safety: 3.04, Privacy: 9.120000000000001
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: In circumstances where an application holds important data client-side in tokens (cookies, URLs, data files, and so forth) that data can be manipulated. If client or server-side application components...

- Using Alternative IP Address Encodings
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.0
  Risk Scores: Financial: 2.2800000000000002, Safety: 2.2800000000000002, Privacy: 9.120000000000001
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: This attack relies on the adversary using unexpected formats for representing IP addresses. Networked applications may expect network location information in a specific format, such as fully qualified...

- Exploiting Multiple Input Interpretation Layers
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.0
  Risk Scores: Financial: 2.2800000000000002, Safety: 2.2800000000000002, Privacy: 9.120000000000001
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: An attacker supplies the target software with input data that contains sequences of special characters designed to bypass input validation logic. This exploit relies on the target making multiples pas...

- Development Alteration
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.0
  Risk Scores: Financial: 2.2800000000000002, Safety: 2.2800000000000002, Privacy: 9.120000000000001
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: An adversary modifies a technology, product, or component during its development to acheive a negative impact once the system is deployed. The goal of the adversary is to modify the system in such a w...

- Malicious Logic Insertion into Product Software via Configuration Management Manipulation
  Impact Scores: Financial: 4.0, Safety: 1, Privacy: 1
  Risk Scores: Financial: 9.120000000000001, Safety: 2.2800000000000002, Privacy: 2.2800000000000002
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: An adversary exploits a configuration management system so that malicious logic is inserted into a software products build, update or deployed environment. If an adversary can control the elements inc...

- Design Alteration
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.0

Risk Scores: Financial: 2.2800000000000002, Safety: 2.2800000000000002, Privacy: 9.120000000000001
Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
Description: An adversary modifies the design of a technology, product, or component to acheive a negative impact once the system is deployed. In this type of attack, the goal of the adversary is to modify the des...

- Contradictory Destinations in Traffic Routing Schemes
  Impact Scores: Financial: 4.0, Safety: 1, Privacy: 1
  Risk Scores: Financial: 9.120000000000001, Safety: 2.2800000000000002, Privacy: 2.2800000000000002
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: Adversaries can provide contradictory destinations when sending messages. Traffic is routed in networks using the domain names in various headers available at different levels of the OSI model. In a C...

- Object Injection
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.0
  Risk Scores: Financial: 2.2800000000000002, Safety: 2.2800000000000002, Privacy: 9.120000000000001
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: An adversary attempts to exploit an application by injecting additional, malicious content during its processing of serialized objects. Developers leverage serialization in order to convert data or st...

- Bluetooth Impersonation AttackS (BIAS)
  Impact Scores: Financial: 4.0, Safety: 1, Privacy: 1
  Risk Scores: Financial: 9.120000000000001, Safety: 2.2800000000000002, Privacy: 2.2800000000000002
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: An adversary disguises the MAC address of their Bluetooth enabled device to one for which there exists an active and trusted connection and authenticates successfully. The adversary can then perform m...

- Alteration of a Software Update
  Impact Scores: Financial: 4.0, Safety: 1, Privacy: 1
  Risk Scores: Financial: 9.120000000000001, Safety: 2.2800000000000002, Privacy: 2.2800000000000002
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: An adversary with access to an organization’s software update infrastructure inserts malware into the content of an outgoing update to fielded systems where a wide range of malicious effects are possi...

- Eavesdropping on a Monitor
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.0
  Risk Scores: Financial: 2.2800000000000002, Safety: 2.2800000000000002, Privacy: 9.120000000000001
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: An Adversary can eavesdrop on the content of an external monitor through the air without modifying any cable or installing software, just capturing this signal emitted by the cable or video port, with...

- Browser in the Middle (BiTM)
  Impact Scores: Financial: 4.0, Safety: 1, Privacy: 1
  Risk Scores: Financial: 9.120000000000001, Safety: 2.2800000000000002, Privacy: 2.2800000000000002
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: An adversary exploits the inherent functionalities of a web browser, in order to establish an unnoticed remote desktop connection in the victim's browser to the adversary's system. The adversary must ...

- Manipulating State
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.0
  Risk Scores: Financial: 2.2800000000000002, Safety: 2.2800000000000002, Privacy: 9.120000000000001
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: The adversary modifies state information maintained by the target software or causes a state transition in hardware. If successful, the target will use this tainted state and execute in an unintended ...

- Escaping a Sandbox by Calling Code in Another Language
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5
  Risk Scores: Financial: 1.52, Safety: 1.52, Privacy: 7.6
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: The attacker may submit malicious code of another language to obtain access to privileges that were not intentionally exposed by the sandbox, thus escaping the sandbox. For instance, Java code cannot ...

- Hijacking a Privileged Thread of Execution
  Impact Scores: Financial: 5, Safety: 1, Privacy: 1
  Risk Scores: Financial: 7.6, Safety: 1.52, Privacy: 1.52
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: An adversary hijacks a privileged thread of execution by injecting malicious code into a running process. By using a privleged thread to do their bidding, adversaries can evade process-based detection...

- Subvert Code-signing Facilities
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5
  Risk Scores: Financial: 1.52, Safety: 1.52, Privacy: 7.6
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: Many languages use code signing facilities to vouch for code's identity and to thus tie code to its assigned privileges within an environment. Subverting this mechanism can be instrumental in an attac...

- Load Value Injection
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5
  Risk Scores: Financial: 1.52, Safety: 1.52, Privacy: 7.6
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: An adversary exploits a hardware design flaw in a CPU implementation of transient instruction execution in which a faulting or assisted load instruction transiently forwards adversary-controlled data ...

- Interface Manipulation
  Impact Scores: Financial: 3.0, Safety: 1, Privacy: 1
  Risk Scores: Financial: 6.840000000000001, Safety: 2.2800000000000002, Privacy: 2.2800000000000002
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: An adversary manipulates the use or processing of an interface (e.g. Application Programming Interface (API) or System-on-Chip (SoC)) resulting in an adverse impact upon the security of the system imp...

- Parameter Injection
  Impact Scores: Financial: 1, Safety: 1, Privacy: 3.0
  Risk Scores: Financial: 2.2800000000000002, Safety: 2.2800000000000002, Privacy: 6.840000000000001
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: An adversary manipulates the content of request parameters for the purpose of undermining the security of the target. Some parameter encodings use text characters as separators. For example, parameter...

- Content Spoofing
  Impact Scores: Financial: 3.0, Safety: 1, Privacy: 3.0
  Risk Scores: Financial: 6.840000000000001, Safety: 2.2800000000000002, Privacy: 6.840000000000001
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: An adversary modifies content to make it contain something other than what the original content producer intended while keeping the apparent source of the content unchanged. The term content spoofing ...

- Resource Location Spoofing
  Impact Scores: Financial: 1, Safety: 1, Privacy: 3.0
  Risk Scores: Financial: 2.2800000000000002, Safety: 2.2800000000000002, Privacy: 6.840000000000001
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20

Description: An adversary deceives an application or user and convinces them to request a resource from an unintended location. By spoofing the location, the adversary can cause an alternate resource to be used, o...

- Cross-Site Flashing
  Impact Scores: Financial: 3.0, Safety: 1, Privacy: 1
  Risk Scores: Financial: 6.840000000000001, Safety: 2.2800000000000002, Privacy: 2.2800000000000002
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: An attacker is able to trick the victim into executing a Flash document that passes commands or calls to a Flash player browser plugin, allowing the attacker to exploit native Flash functionality in t...

- Modification of Registry Run Keys
  Impact Scores: Financial: 1, Safety: 1, Privacy: 3.0
  Risk Scores: Financial: 2.2800000000000002, Safety: 2.2800000000000002, Privacy: 6.840000000000001
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: An adversary adds a new entry to the run keys in the Windows registry so that an application of their choosing is executed when a user logs in. In this way, the adversary can get their executable to o...

- Using Leading 'Ghost' Character Sequences to Bypass Input Filters
  Impact Scores: Financial: 1, Safety: 1, Privacy: 3.0
  Risk Scores: Financial: 2.2800000000000002, Safety: 2.2800000000000002, Privacy: 6.840000000000001
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: Some APIs will strip certain leading characters from a string of parameters. An adversary can intentionally introduce leading ghost characters (extra characters that don't affect the validity of the r...

- Manipulate Human Behavior
  Impact Scores: Financial: 1, Safety: 1, Privacy: 3.0
  Risk Scores: Financial: 2.2800000000000002, Safety: 2.2800000000000002, Privacy: 6.840000000000001
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: An adversary exploits inherent human psychological predisposition to influence a targeted individual or group to solicit information or manipulate the target into performing an action that serves the ...

- Disable Security Software
  Impact Scores: Financial: 3.0, Safety: 1, Privacy: 1
  Risk Scores: Financial: 6.840000000000001, Safety: 2.2800000000000002, Privacy: 2.2800000000000002
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: An adversary exploits a weakness in access control to disable security tools so that detection does not occur. This can take the form of killing processes, deleting registry keys so that tools do not ...

- Collect Data from Registries
  Impact Scores: Financial: 1, Safety: 1, Privacy: 3.0
  Risk Scores: Financial: 2.2800000000000002, Safety: 2.2800000000000002, Privacy: 6.840000000000001
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: An adversary exploits a weakness in authorization to gather system-specific data and sensitive information within a registry (e.g., Windows Registry, Mac plist). These contain information about the sy...

- Collect Data from Screen Capture
  Impact Scores: Financial: 1, Safety: 1, Privacy: 3.0
  Risk Scores: Financial: 2.2800000000000002, Safety: 2.2800000000000002, Privacy: 6.840000000000001
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: An adversary gathers sensitive information by exploiting the system's screen capture functionality. Through screenshots, the adversary aims to see what happens on the screen over the course of an oper...

- Retrieve Data from Decommissioned Devices

Impact Scores: Financial: 1, Safety: 1, Privacy: 3.0
Risk Scores: Financial: 2.2800000000000002, Safety: 2.2800000000000002, Privacy: 6.840000000000001
Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
Description: An adversary obtains decommissioned, recycled, or discarded systems and devices that can include an organization’s intellectual property, employee data, and other types of controlled information. Syst...

- Web Application Fingerprinting
  Impact Scores: Financial: 1, Safety: 1, Privacy: 2.0
  Risk Scores: Financial: 3.04, Safety: 3.04, Privacy: 6.08
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: An attacker sends a series of probes to a web application in order to elicit version-dependent and type-dependent behavior that assists in identifying the target. An attacker could learn information s...

- Fuzzing for application mapping
  Impact Scores: Financial: 1, Safety: 2.0, Privacy: 1
  Risk Scores: Financial: 3.04, Safety: 6.08, Privacy: 3.04
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: An attacker sends random, malformed, or otherwise unexpected messages to a target application and observes the application's log or error messages returned. The attacker does not initially know how a ...

- Forced Deadlock
  Impact Scores: Financial: 4.0, Safety: 1, Privacy: 1
  Risk Scores: Financial: 6.08, Safety: 1.52, Privacy: 1.52
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: The adversary triggers and exploits a deadlock condition in the target software to cause a denial of service. A deadlock can occur when two or more competing actions are waiting for each other to fini...

- Schema Poisoning
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.0
  Risk Scores: Financial: 1.52, Safety: 1.52, Privacy: 6.08
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: An adversary corrupts or modifies the content of a schema for the purpose of undermining the security of the target. Schemas provide the structure and content definitions for resources used by an appl...

- USB Memory Attacks
  Impact Scores: Financial: 2.0, Safety: 1, Privacy: 4.0
  Risk Scores: Financial: 3.04, Safety: 1.52, Privacy: 6.08
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: An adversary loads malicious code onto a USB memory stick in order to infect any system which the device is plugged in to. USB drives present a significant security risk for business and government ag...

- Signature Spoofing by Misrepresentation
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.0
  Risk Scores: Financial: 1.52, Safety: 1.52, Privacy: 6.08
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: An attacker exploits a weakness in the parsing or display code of the recipient software to generate a data blob containing a supposedly valid signature, but the signer's identity is falsely represent...

- Hardware Component Substitution During Baselining
  Impact Scores: Financial: 4.0, Safety: 1, Privacy: 1
  Risk Scores: Financial: 6.08, Safety: 1.52, Privacy: 1.52
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: An adversary with access to system components during allocated baseline development can substitute a

maliciously altered hardware component for a baseline component during the product development and ...

- Malicious Hardware Update
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.0
  Risk Scores: Financial: 1.52, Safety: 1.52, Privacy: 6.08
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: An adversary introduces malicious hardware during an update or replacement procedure, allowing for additional compromise or site disruption at the victim location. After deployment, it is not uncommon...

- Open-Source Library Manipulation
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.0
  Risk Scores: Financial: 1.52, Safety: 1.52, Privacy: 6.08
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: Adversaries implant malicious code in open source software (OSS) libraries to have it widely distributed, as OSS is commonly downloaded by developers and other users to incorporate into software devel...

- ASIC With Malicious Functionality
  Impact Scores: Financial: 4.0, Safety: 1, Privacy: 1
  Risk Scores: Financial: 6.08, Safety: 1.52, Privacy: 1.52
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: An attacker with access to the development environment process of an application-specific integrated circuit (ASIC) for a victim system being developed or maintained after initial deployment can inser...

- Hardware Fault Injection
  Impact Scores: Financial: 1, Safety: 4.0, Privacy: 4.0
  Risk Scores: Financial: 1.52, Safety: 6.08, Privacy: 6.08
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: The adversary uses disruptive signals or events, or alters the physical environment a device operates in, to cause faulty behavior in electronic devices. This can include electromagnetic pulses, laser...

- Carry-Off GPS Attack
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.0
  Risk Scores: Financial: 1.52, Safety: 1.52, Privacy: 6.08
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: A common form of a GPS spoofing attack, commonly termed a carry-off attack begins with an adversary broadcasting signals synchronized with the genuine signals observed by the target receiver. The powe...

- DLL Side-Loading
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.0
  Risk Scores: Financial: 1.52, Safety: 1.52, Privacy: 6.08
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: An adversary places a malicious version of a Dynamic-Link Library (DLL) in the Windows Side-by-Side (WinSxS) directory to trick the operating system into loading this malicious DLL instead of a legiti...

- Use of Captured Tickets (Pass The Ticket)
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.0
  Risk Scores: Financial: 1.52, Safety: 1.52, Privacy: 6.08
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: An adversary uses stolen Kerberos tickets to access systems/resources that leverage the Kerberos authentication protocol. The Kerberos authentication protocol centers around a ticketing system which i...

- Sniff Application Code
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.0

Risk Scores: Financial: 1.52, Safety: 1.52, Privacy: 6.08
Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
Description: An adversary passively sniffs network communications and captures application code bound for an authorized client. Once obtained, they can use it as-is, or through reverse-engineering glean sensitive ...

- Key Negotiation of Bluetooth Attack (KNOB)
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.0
  Risk Scores: Financial: 1.52, Safety: 1.52, Privacy: 6.08
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: An adversary can exploit a flaw in Bluetooth key negotiation allowing them to decrypt information sent between two devices communicating via Bluetooth. The adversary uses an Adversary in the Middle se...

- Malicious Code Implanted During Chip Programming
  Impact Scores: Financial: 4.0, Safety: 1, Privacy: 1
  Risk Scores: Financial: 6.08, Safety: 1.52, Privacy: 1.52
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: During the programming step of chip manufacture, an adversary with access and necessary technical skills maliciously alters a chip’s intended program logic to produce an effect intended by the adversa...

- AJAX Footprinting
  Impact Scores: Financial: 1, Safety: 1, Privacy: 2.0
  Risk Scores: Financial: 3.04, Safety: 3.04, Privacy: 6.08
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: This attack utilizes the frequent client-server roundtrips in Ajax conversation to scan a system. While Ajax does not open up new vulnerabilities per se, it does optimize them from an attacker point o...

- Interception
  Impact Scores: Financial: 1, Safety: 1, Privacy: 3.0
  Risk Scores: Financial: 1.52, Safety: 1.52, Privacy: 4.5600000000000005
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: An adversary monitors data streams to or from the target for information gathering purposes. This attack may be undertaken to solely gather sensitive information or to support a further attack against...

- XML Ping of the Death
  Impact Scores: Financial: 1, Safety: 3.0, Privacy: 1
  Risk Scores: Financial: 1.52, Safety: 4.5600000000000005, Privacy: 1.52
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: An attacker initiates a resource depletion attack where a large number of small XML messages are delivered at a sufficiently rapid rate to cause a denial of service or crash of the target. Transaction...

- Active OS Fingerprinting
  Impact Scores: Financial: 1, Safety: 1, Privacy: 2.0
  Risk Scores: Financial: 2.2800000000000002, Safety: 2.2800000000000002, Privacy: 4.5600000000000005
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: An adversary engages in activity to detect the operating system or firmware version of a remote target by interrogating a device, server, or platform with a probe designed to solicit behavior that wil...

- TCP Timestamp Probe
  Impact Scores: Financial: 2.0, Safety: 1, Privacy: 1
  Risk Scores: Financial: 4.5600000000000005, Safety: 2.2800000000000002, Privacy: 2.2800000000000002
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: This OS fingerprinting probe examines the remote server's implementation of TCP timestamps. Not all operating systems implement timestamps within the TCP header, but when timestamps are used then this...

- TCP Sequence Number Probe
  Impact Scores: Financial: 2.0, Safety: 1, Privacy: 1
  Risk Scores: Financial: 4.5600000000000005, Safety: 2.2800000000000002, Privacy: 2.2800000000000002
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: This OS fingerprinting probe tests the target system's assignment of TCP sequence numbers. One common way to test TCP Sequence Number generation is to send a probe packet to an open port on the target...

- TCP (ISN) Greatest Common Divisor Probe
  Impact Scores: Financial: 1, Safety: 1, Privacy: 2.0
  Risk Scores: Financial: 2.2800000000000002, Safety: 2.2800000000000002, Privacy: 4.5600000000000005
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: This OS fingerprinting probe sends a number of TCP SYN packets to an open port of a remote machine. The Initial Sequence Number (ISN) in each of the SYN/ACK response packets is analyzed to determine t...

- TCP (ISN) Counter Rate Probe
  Impact Scores: Financial: 1, Safety: 1, Privacy: 2.0
  Risk Scores: Financial: 2.2800000000000002, Safety: 2.2800000000000002, Privacy: 4.5600000000000005
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: This OS detection probe measures the average rate of initial sequence number increments during a period of time. Sequence numbers are incremented using a time-based algorithm and are susceptible to a ...

- TCP (ISN) Sequence Predictability Probe
  Impact Scores: Financial: 1, Safety: 1, Privacy: 2.0
  Risk Scores: Financial: 2.2800000000000002, Safety: 2.2800000000000002, Privacy: 4.5600000000000005
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: This type of operating system probe attempts to determine an estimate for how predictable the sequence number generation algorithm is for a remote host. Statistical techniques, such as standard deviat...

- TCP Initial Window Size Probe
  Impact Scores: Financial: 2.0, Safety: 1, Privacy: 1
  Risk Scores: Financial: 4.5600000000000005, Safety: 2.2800000000000002, Privacy: 2.2800000000000002
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: This OS fingerprinting probe checks the initial TCP Window size. TCP stacks limit the range of sequence numbers allowable within a session to maintain the connected state within TCP protocol logic. Th...

- TCP Options Probe
  Impact Scores: Financial: 2.0, Safety: 1, Privacy: 1
  Risk Scores: Financial: 4.5600000000000005, Safety: 2.2800000000000002, Privacy: 2.2800000000000002
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: This OS fingerprinting probe analyzes the type and order of any TCP header options present within a response segment. Most operating systems use unique ordering and different option sets when options ...

- Pretexting
  Impact Scores: Financial: 1, Safety: 1, Privacy: 2.0
  Risk Scores: Financial: 2.2800000000000002, Safety: 2.2800000000000002, Privacy: 4.5600000000000005
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: An adversary engages in pretexting behavior to solicit information from target persons, or manipulate the target into performing some action that serves the adversary's interests. During a pretexting ...

- Incomplete Data Deletion in a Multi-Tenant Environment
  Impact Scores: Financial: 1, Safety: 1, Privacy: 3.0
  Risk Scores: Financial: 1.52, Safety: 1.52, Privacy: 4.5600000000000005
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20

Description: An adversary obtains unauthorized information due to insecure or incomplete data deletion in a multi-tenant environment. If a cloud provider fails to completely delete storage and data from former clo...

- Adding a Space to a File Extension
  Impact Scores: Financial: 1, Safety: 1, Privacy: 3.0
  Risk Scores: Financial: 1.52, Safety: 1.52, Privacy: 4.5600000000000005
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: An adversary adds a space character to the end of a file extension and takes advantage of an application that does not properly neutralize trailing special elements in file names. This extra space, wh...

- Reverse Engineering
  Impact Scores: Financial: 2.0, Safety: 1, Privacy: 1
  Risk Scores: Financial: 3.04, Safety: 1.52, Privacy: 1.52
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: An adversary discovers the structure, function, and composition of an object, resource, or system by using a variety of analysis techniques to effectively determine how the analyzed entity was constru...

- Fingerprinting
  Impact Scores: Financial: 1, Safety: 1, Privacy: 1
  Risk Scores: Financial: 3.04, Safety: 3.04, Privacy: 3.04
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: An adversary compares output from a target system to known indicators that uniquely identify specific details about the target. Most commonly, fingerprinting is done to determine operating system and ...

- Target Influence via Framing
  Impact Scores: Financial: 1, Safety: 1, Privacy: 2.0
  Risk Scores: Financial: 1.52, Safety: 1.52, Privacy: 3.04
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: An adversary uses framing techniques to contextualize a conversation so that the target is more likely to be influenced by the adversary's point of view. Framing is information and experiences in life...

- Influence via Psychological Principles
  Impact Scores: Financial: 2.0, Safety: 1, Privacy: 1
  Risk Scores: Financial: 3.04, Safety: 1.52, Privacy: 1.52
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: The adversary shapes the target's actions or behavior by focusing on the ways human interact and learn, leveraging such elements as cognitive and social psychology. In a variety of ways, a target can ...

- Process Footprinting
  Impact Scores: Financial: 1, Safety: 1, Privacy: 2.0
  Risk Scores: Financial: 1.52, Safety: 1.52, Privacy: 3.04
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: An adversary exploits functionality meant to identify information about the currently running processes on the target system to an authorized user. By knowing what processes are running on the target ...

- Services Footprinting
  Impact Scores: Financial: 1, Safety: 1, Privacy: 2.0
  Risk Scores: Financial: 1.52, Safety: 1.52, Privacy: 3.04
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: An adversary exploits functionality meant to identify information about the services on the target system to an authorized user. By knowing what services are registered on the target system, the adver...

- Account Footprinting

Impact Scores: Financial: 1, Safety: 1, Privacy: 2.0
Risk Scores: Financial: 1.52, Safety: 1.52, Privacy: 3.04
Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
Description: An adversary exploits functionality meant to identify information about the domain accounts and their permissions on the target system to an authorized user. By knowing what accounts are registered on...

- Group Permission Footprinting
Impact Scores: Financial: 1, Safety: 1, Privacy: 2.0
Risk Scores: Financial: 1.52, Safety: 1.52, Privacy: 3.04
Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
Description: An adversary exploits functionality meant to identify information about user groups and their permissions on the target system to an authorized user. By knowing what users/permissions are registered o...

- Owner Footprinting
Impact Scores: Financial: 1, Safety: 1, Privacy: 2.0
Risk Scores: Financial: 1.52, Safety: 1.52, Privacy: 3.04
Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
Description: An adversary exploits functionality meant to identify information about the primary users on the target system to an authorized user. They may do this, for example, by reviewing logins or file modific...

- System Footprinting
Impact Scores: Financial: 1, Safety: 1, Privacy: 2.0
Risk Scores: Financial: 1.52, Safety: 1.52, Privacy: 3.04
Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
Description: An adversary engages in active probing and exploration activities to determine security information about a remote target system. Often times adversaries will rely on remote applications that can be p...

- Collect Data from Clipboard
Impact Scores: Financial: 1, Safety: 1, Privacy: 2.0
Risk Scores: Financial: 1.52, Safety: 1.52, Privacy: 3.04
Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
Description: The adversary exploits an application that allows for the copying of sensitive data or information by collecting information copied to the clipboard. Data copied to the clipboard can be accessed by ot...

Component: Wheel Speed Sensor

Type: Sensor
Safety Level: ASIL B
Interfaces: CAN
Access Points:
Data Types: Sensor Data
Location: External
Trust Zone: Untrusted
Connected To: ECU003

Identified Threats:

- Buffer Manipulation
Impact Scores: Financial: 1, Safety: 1, Privacy: 5
Risk Scores: Financial: 3.04, Safety: 3.04, Privacy: 15.2
Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20

Description: An adversary manipulates an application's interaction with a buffer in an attempt to read or modify data they shouldn't have access to. Buffer attacks are distinguished in that it is the buffer space ...

- Redirect Access to Libraries
  Impact Scores: Financial: 1, Safety: 5, Privacy: 1
  Risk Scores: Financial: 3.04, Safety: 15.2, Privacy: 3.04
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: An adversary exploits a weakness in the way an application searches for external libraries to manipulate the execution flow to point to an adversary supplied library or code base. This pattern of atta...

- XSS Targeting Non-Script Elements
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5
  Risk Scores: Financial: 3.04, Safety: 3.04, Privacy: 15.2
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: This attack is a form of Cross-Site Scripting (XSS) where malicious scripts are embedded in elements that are not expected to host scripts such as image tags (<img>), comments in XML documents (< !-CD...

- Retrieve Embedded Sensitive Data
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5
  Risk Scores: Financial: 3.04, Safety: 3.04, Privacy: 15.2
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: An attacker examines a target system to find sensitive data that has been embedded within it. This information can reveal confidential contents, such as account numbers or individual keys/credentials ...

- Leveraging/Manipulating Configuration File Search Paths
  Impact Scores: Financial: 5, Safety: 1, Privacy: 1
  Risk Scores: Financial: 15.2, Safety: 3.04, Privacy: 3.04
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: This pattern of attack sees an adversary load a malicious resource into a program's standard path so that when a known command is executed then the system instead executes the malicious component. The...

- Manipulating Writeable Terminal Devices
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5
  Risk Scores: Financial: 3.04, Safety: 3.04, Privacy: 15.2
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: This attack exploits terminal devices that allow themselves to be written to by other users. The attacker sends command strings to the target terminal device hoping that the target user will hit enter...

- Overflow Binary Resource File
  Impact Scores: Financial: 5, Safety: 1, Privacy: 1
  Risk Scores: Financial: 15.2, Safety: 3.04, Privacy: 3.04
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: An attack of this type exploits a buffer overflow vulnerability in the handling of binary resources. Binary resources may include music files like MP3, image files like JPEG files, and any other binar...

- Poison Web Service Registry
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5
  Risk Scores: Financial: 3.04, Safety: 3.04, Privacy: 15.2
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: SOA and Web Services often use a registry to perform look up, get schema information, and metadata about services. A poisoned registry can redirect (think phishing for servers) the service requester t...

- String Format Overflow in syslog()

Impact Scores: Financial: 1, Safety: 1, Privacy: 5
Risk Scores: Financial: 3.04, Safety: 3.04, Privacy: 15.2
Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
Description: This attack targets applications and software that uses the syslog() function insecurely. If an application does not explicitely use a format string parameter in a call to syslog(), user input can be ...

- Manipulating User-Controlled Variables
Impact Scores: Financial: 2.0, Safety: 1, Privacy: 5
Risk Scores: Financial: 6.08, Safety: 3.04, Privacy: 15.2
Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
Description: This attack targets user controlled variables (DEBUG=1, PHP Globals, and So Forth). An adversary can override variables leveraging user-supplied, untrusted query variables directly used on the applica...

- XQuery Injection
Impact Scores: Financial: 1, Safety: 1, Privacy: 5
Risk Scores: Financial: 3.04, Safety: 3.04, Privacy: 15.2
Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
Description: This attack utilizes XQuery to probe and attack server systems; in a similar manner that SQL Injection allows an attacker to exploit SQL calls to RDBMS, XQuery Injection uses improperly validated data...

- Pharming
Impact Scores: Financial: 1, Safety: 1, Privacy: 5
Risk Scores: Financial: 3.04, Safety: 3.04, Privacy: 15.2
Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
Description: A pharming attack occurs when the victim is fooled into entering sensitive data into supposedly trusted locations, such as an online bank site or a trading platform. An attacker can impersonate these ...

- Phishing
Impact Scores: Financial: 1, Safety: 1, Privacy: 5
Risk Scores: Financial: 3.04, Safety: 3.04, Privacy: 15.2
Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
Description: Phishing is a social engineering technique where an attacker masquerades as a legitimate entity with which the victim might do business in order to prompt the user to reveal some confidential informat...

- Accessing Functionality Not Properly Constrained by ACLs
Impact Scores: Financial: 1, Safety: 1, Privacy: 4.0
Risk Scores: Financial: 3.04, Safety: 3.04, Privacy: 12.16
Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
Description: In applications, particularly web applications, access to functionality is mitigated by an authorization framework. This framework maps Access Control Lists (ACLs) to elements of the application's fun...

- Buffer Overflow via Environment Variables
Impact Scores: Financial: 4.0, Safety: 1, Privacy: 1
Risk Scores: Financial: 12.16, Safety: 3.04, Privacy: 3.04
Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
Description: This attack pattern involves causing a buffer overflow through manipulation of environment variables. Once the adversary finds that they can modify an environment variable, they may try to overflow as...

- Server Side Include (SSI) Injection
Impact Scores: Financial: 1, Safety: 1, Privacy: 4.0
Risk Scores: Financial: 3.04, Safety: 3.04, Privacy: 12.16
Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
Description: An attacker can use Server Side Include (SSI) Injection to send code to a web application that then gets

executed by the web server. Doing so enables the attacker to achieve similar results to Cross S...

- Format String Injection
  Impact Scores: Financial: 1, Safety: 2.0, Privacy: 4.0
  Risk Scores: Financial: 3.04, Safety: 6.08, Privacy: 12.16
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: An adversary includes formatting characters in a string input field on the target application. Most applications assume that users will provide static text and may respond unpredictably to the presenc...

- Cache Poisoning
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.0
  Risk Scores: Financial: 3.04, Safety: 3.04, Privacy: 12.16
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: An attacker exploits the functionality of cache technologies to cause specific data to be cached that aids the attackers' objectives. This describes any attack whereby an attacker places incorrect or ...

- DNS Cache Poisoning
  Impact Scores: Financial: 4.0, Safety: 1, Privacy: 1
  Risk Scores: Financial: 12.16, Safety: 3.04, Privacy: 3.04
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: A domain name server translates a domain name (such as www.example.com) into an IP address that Internet hosts use to contact Internet resources. An adversary modifies a public DNS cache to cause cert...

- Command Delimiters
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.0
  Risk Scores: Financial: 3.04, Safety: 3.04, Privacy: 12.16
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: An attack of this type exploits a programs' vulnerabilities that allows an attacker's commands to be concatenated onto a legitimate command with the intent of targeting other resources such as the fil...

- Malicious Automated Software Update via Redirection
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.0
  Risk Scores: Financial: 3.04, Safety: 3.04, Privacy: 12.16
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: An attacker exploits two layers of weaknesses in server or client software for automated update mechanisms to undermine the integrity of the target code-base. The first weakness involves a failure to ...

- PHP Remote File Inclusion
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.0
  Risk Scores: Financial: 3.04, Safety: 3.04, Privacy: 12.16
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: In this pattern the adversary is able to load and execute arbitrary code remotely available from the application. This is usually accomplished through an insecurely configured PHP runtime environment ...

- XSS Using Alternate Syntax
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.0
  Risk Scores: Financial: 3.04, Safety: 3.04, Privacy: 12.16
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: An adversary uses alternate forms of keywords or commands that result in the same action as the primary form but which may not be caught by filters. For example, many keywords are processed in a case ...

- Serialized Data External Linking
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.0

Risk Scores: Financial: 3.04, Safety: 3.04, Privacy: 12.16
Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
Description: An adversary creates a serialized data file (e.g. XML, YAML, etc...) that contains an external data reference. Because serialized data parsers may not validate documents with external references, ther...

- Leveraging Race Conditions
  Impact Scores: Financial: 4.0, Safety: 1, Privacy: 1
  Risk Scores: Financial: 12.16, Safety: 3.04, Privacy: 3.04
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: The adversary targets a race condition occurring when multiple processes access and manipulate the same resource concurrently, and the outcome of the execution depends on the particular order in which...

- Leveraging Time-of-Check and Time-of-Use (TOCTOU) Race Conditions
  Impact Scores: Financial: 4.0, Safety: 1, Privacy: 1
  Risk Scores: Financial: 12.16, Safety: 3.04, Privacy: 3.04
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: This attack targets a race condition occurring between the time of check (state) for a resource and the time of use of a resource. A typical example is file access. The adversary can leverage a file a...

- Using Meta-characters in E-mail Headers to Inject Malicious Payloads
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.0
  Risk Scores: Financial: 3.04, Safety: 3.04, Privacy: 12.16
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: This type of attack involves an attacker leveraging meta-characters in email headers to inject improper behavior into email programs. Email software has become increasingly sophisticated and feature-r...

- Buffer Overflow via Symbolic Links
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.0
  Risk Scores: Financial: 3.04, Safety: 3.04, Privacy: 12.16
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: This type of attack leverages the use of symbolic links to cause buffer overflows. An adversary can try to create or manipulate a symbolic link file such that its contents result in out of bounds data...

- Passing Local Filenames to Functions That Expect a URL
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.0
  Risk Scores: Financial: 3.04, Safety: 3.04, Privacy: 12.16
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: This attack relies on client side code to access local files and resources instead of URLs. When the client browser is expecting a URL string, but instead receives a request for a local file, that exe...

- Session Credential Falsification through Prediction
  Impact Scores: Financial: 4.0, Safety: 1, Privacy: 1
  Risk Scores: Financial: 12.16, Safety: 3.04, Privacy: 3.04
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: This attack targets predictable session ID in order to gain privileges. The attacker can predict the session ID used during a transaction to perform spoofing and session hijacking....

- Using Slashes and URL Encoding Combined to Bypass Validation Logic
  Impact Scores: Financial: 4.0, Safety: 1, Privacy: 1
  Risk Scores: Financial: 12.16, Safety: 3.04, Privacy: 3.04
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: This attack targets the encoding of the URL combined with the encoding of the slash characters. An attacker can take advantage of the multiple ways of encoding a URL and abuse the interpretation of th...

- Voice Phishing
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.0
  Risk Scores: Financial: 3.04, Safety: 3.04, Privacy: 12.16
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: An adversary targets users with a phishing attack for the purpose of soliciting account passwords or sensitive information from the user. Voice Phishing is a variation of the Phishing social engineeri...

- Malicious Automated Software Update via Spoofing
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.0
  Risk Scores: Financial: 3.04, Safety: 3.04, Privacy: 12.16
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: An attackers uses identify or content spoofing to trick a client into performing an automated software update from a malicious source. A malicious automated software update that leverages spoofing can...

- Blind SQL Injection
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.0
  Risk Scores: Financial: 3.04, Safety: 3.04, Privacy: 12.16
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: Blind SQL Injection results from an insufficient mitigation for SQL Injection. Although suppressing database error messages are considered best practice, the suppression alone is not sufficient to pre...

- URL Encoding
  Impact Scores: Financial: 4.0, Safety: 1, Privacy: 1
  Risk Scores: Financial: 12.16, Safety: 3.04, Privacy: 3.04
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: This attack targets the encoding of the URL. An adversary can take advantage of the multiple way of encoding an URL and abuse the interpretation of the URL....

- User-Controlled Filename
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.0
  Risk Scores: Financial: 3.04, Safety: 3.04, Privacy: 12.16
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: An attack of this type involves an adversary inserting malicious characters (such as a XSS redirection) into a filename, directly or indirectly that is then used by the target software to generate HTM...

- Using Escaped Slashes in Alternate Encoding
  Impact Scores: Financial: 4.0, Safety: 1, Privacy: 1
  Risk Scores: Financial: 12.16, Safety: 3.04, Privacy: 3.04
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: This attack targets the use of the backslash in alternate encoding. An adversary can provide a backslash as a leading character and causes a parser to believe that the next character is special. This ...

- Buffer Overflow in an API Call
  Impact Scores: Financial: 4.0, Safety: 1, Privacy: 1
  Risk Scores: Financial: 12.16, Safety: 3.04, Privacy: 3.04
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: This attack targets libraries or shared code modules which are vulnerable to buffer overflow attacks. An adversary who has knowledge of known vulnerable libraries or shared code can easily target soft...

- Using UTF-8 Encoding to Bypass Validation Logic
  Impact Scores: Financial: 1, Safety: 4.0, Privacy: 1
  Risk Scores: Financial: 3.04, Safety: 12.16, Privacy: 3.04
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20

Description: This attack is a specific variation on leveraging alternate encodings to bypass validation logic. This attack leverages the possibility to encode potentially harmful input in UTF-8 and submit it to ap...

- XPath Injection
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.0
  Risk Scores: Financial: 3.04, Safety: 3.04, Privacy: 12.16
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: An attacker can craft special user-controllable input consisting of XPath expressions to inject the XML database and bypass authentication or glean information that they normally would not be able to....

- OS Command Injection
  Impact Scores: Financial: 4.0, Safety: 1, Privacy: 1
  Risk Scores: Financial: 12.16, Safety: 3.04, Privacy: 3.04
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: In this type of an attack, an adversary injects operating system commands into existing application functions. An application that uses untrusted input to build command strings is vulnerable. An adver...

- Buffer Overflow in Local Command-Line Utilities
  Impact Scores: Financial: 4.0, Safety: 1, Privacy: 1
  Risk Scores: Financial: 12.16, Safety: 3.04, Privacy: 3.04
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: This attack targets command-line utilities available in a number of shells. An adversary can leverage a vulnerability found in a command-line utility to escalate privilege to root....

- Reflection Attack in Authentication Protocol
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.0
  Risk Scores: Financial: 3.04, Safety: 3.04, Privacy: 12.16
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: An adversary can abuse an authentication protocol susceptible to reflection attack in order to defeat it. Doing so allows the adversary illegitimate access to the target system, without possessing the...

- Forced Integer Overflow
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.0
  Risk Scores: Financial: 3.04, Safety: 3.04, Privacy: 12.16
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: This attack forces an integer variable to go out of range. The integer variable is often used as an offset such as size of memory allocation or similarly. The attacker would typically control the valu...

- WSDL Scanning
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.0
  Risk Scores: Financial: 3.04, Safety: 3.04, Privacy: 12.16
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: This attack targets the WSDL interface made available by a web service. The attacker may scan the WSDL interface to reveal sensitive information about invocation patterns, underlying technology implem...

- Root/Jailbreak Detection Evasion via Debugging
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5
  Risk Scores: Financial: 2.2800000000000002, Safety: 2.2800000000000002, Privacy: 11.400000000000002
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: An adversary inserts a debugger into the program entry point of a mobile application to modify the application binary, with the goal of evading Root/Jailbreak detection. Mobile device users often Root...

- CAN Injection

  Impact Scores: Financial: 3.0, Safety: 4.0, Privacy: 2.0
  Risk Scores: Financial: 6.840000000000001, Safety: 9.120000000000001, Privacy: 4.5600000000000005
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: Manipulation of CAN bus messages leading to vehicle malfunction...

- Sensor Data Manipulation
  Impact Scores: Financial: 3.0, Safety: 4.0, Privacy: 2.0
  Risk Scores: Financial: 6.840000000000001, Safety: 9.120000000000001, Privacy: 4.5600000000000005
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: Tampering with sensor data leading to incorrect vehicle behavior...

- HTTP Request Splitting
  Impact Scores: Financial: 4.0, Safety: 1, Privacy: 1
  Risk Scores: Financial: 9.120000000000001, Safety: 2.2800000000000002, Privacy: 2.2800000000000002
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: An adversary abuses the flexibility and discrepancies in the parsing and interpretation of HTTP Request messages by different intermediary HTTP agents (e.g., load balancer, reverse proxy, web caching ...

- Flooding
  Impact Scores: Financial: 1, Safety: 1, Privacy: 3.0
  Risk Scores: Financial: 3.04, Safety: 3.04, Privacy: 9.120000000000001
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: An adversary consumes the resources of a target by rapidly engaging in a large number of interactions with the target. This type of attack generally exposes a weakness in rate limiting or flow. When s...

- Directory Indexing
  Impact Scores: Financial: 1, Safety: 1, Privacy: 3.0
  Risk Scores: Financial: 3.04, Safety: 3.04, Privacy: 9.120000000000001
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: An adversary crafts a request to a target that results in the target listing/indexing the content of a directory as output. One common method of triggering directory contents as output is to construct...

- Flash Parameter Injection
  Impact Scores: Financial: 1, Safety: 1, Privacy: 3.0
  Risk Scores: Financial: 3.04, Safety: 3.04, Privacy: 9.120000000000001
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: An adversary takes advantage of improper data validation to inject malicious global parameters into a Flash file embedded within an HTML document. Flash files can leverage user-submitted data to confi...

- Exploiting Incorrectly Configured Access Control Security Levels
  Impact Scores: Financial: 1, Safety: 1, Privacy: 3.0
  Risk Scores: Financial: 3.04, Safety: 3.04, Privacy: 9.120000000000001
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: An attacker exploits a weakness in the configuration of access controls and is able to bypass the intended protection that these measures guard against and thereby obtain unauthorized access to the sy...

- Exponential Data Expansion
  Impact Scores: Financial: 1, Safety: 1, Privacy: 3.0
  Risk Scores: Financial: 3.04, Safety: 3.04, Privacy: 9.120000000000001
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: An adversary submits data to a target application which contains nested exponential data expansion to produce excessively large output. Many data format languages allow the definition of macro-like st...

- Inducing Account Lockout
  Impact Scores: Financial: 1, Safety: 1, Privacy: 3.0
  Risk Scores: Financial: 3.04, Safety: 3.04, Privacy: 9.120000000000001
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: An attacker leverages the security functionality of the system aimed at thwarting potential attacks to launch a denial of service attack against a legitimate system user. Many systems, for instance, i...

- XML Routing Detour Attacks
  Impact Scores: Financial: 1, Safety: 1, Privacy: 3.0
  Risk Scores: Financial: 3.04, Safety: 3.04, Privacy: 9.120000000000001
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: An attacker subverts an intermediate system used to process XML content and forces the intermediate to modify and/or re-route the processing of the content. XML Routing Detour Attacks are Adversary in...

- Serialized Data with Nested Payloads
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.0
  Risk Scores: Financial: 2.2800000000000002, Safety: 2.2800000000000002, Privacy: 9.120000000000001
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: Applications often need to transform data in and out of a data format (e.g., XML and YAML) by using a parser. It may be possible for an adversary to inject data that may have an adverse effect on the ...

- Command Injection
  Impact Scores: Financial: 4.0, Safety: 1, Privacy: 1
  Risk Scores: Financial: 9.120000000000001, Safety: 2.2800000000000002, Privacy: 2.2800000000000002
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: An adversary looking to execute a command of their choosing, injects new items into an existing command thus modifying interpretation away from what was intended. Commands in this context are often st...

- Leveraging Race Conditions via Symbolic Links
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.0
  Risk Scores: Financial: 2.2800000000000002, Safety: 2.2800000000000002, Privacy: 9.120000000000001
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: This attack leverages the use of symbolic links (Symlinks) in order to write to sensitive files. An attacker can create a Symlink link to a target file not otherwise accessible to them. When the privi...

- HTTP Response Smuggling
  Impact Scores: Financial: 4.0, Safety: 1, Privacy: 1
  Risk Scores: Financial: 9.120000000000001, Safety: 2.2800000000000002, Privacy: 2.2800000000000002
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: An adversary manipulates and injects malicious content in the form of secret unauthorized HTTP responses, into a single HTTP response from a vulnerable or compromised back-end HTTP agent (e.g., server...

- SOAP Manipulation
  Impact Scores: Financial: 4.0, Safety: 1, Privacy: 1
  Risk Scores: Financial: 9.120000000000001, Safety: 2.2800000000000002, Privacy: 2.2800000000000002
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: Simple Object Access Protocol (SOAP) is used as a communication protocol between a client and server to invoke web services on the server. It is an XML-based protocol, and therefore suffers from many ...

- Fuzzing
  Impact Scores: Financial: 1, Safety: 1, Privacy: 3.0
  Risk Scores: Financial: 3.04, Safety: 3.04, Privacy: 9.120000000000001
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20

Description: In this attack pattern, the adversary leverages fuzzing to try to identify weaknesses in the system. Fuzzing is a software security and functionality testing method that feeds randomly constructed inp...

- HTTP Request Smuggling
  Impact Scores: Financial: 4.0, Safety: 1, Privacy: 1
  Risk Scores: Financial: 9.120000000000001, Safety: 2.2800000000000002, Privacy: 2.2800000000000002
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: An adversary abuses the flexibility and discrepancies in the parsing and interpretation of HTTP Request messages using various HTTP headers, request-line and body parameters as well as message sizes (...

- HTTP Response Splitting
  Impact Scores: Financial: 4.0, Safety: 1, Privacy: 1
  Risk Scores: Financial: 9.120000000000001, Safety: 2.2800000000000002, Privacy: 2.2800000000000002
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: An adversary manipulates and injects malicious content, in the form of secret unauthorized HTTP responses, into a single HTTP response from a vulnerable or compromised back-end HTTP agent (e.g., web s...

- Manipulating Opaque Client-based Data Tokens
  Impact Scores: Financial: 1, Safety: 1, Privacy: 3.0
  Risk Scores: Financial: 3.04, Safety: 3.04, Privacy: 9.120000000000001
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: In circumstances where an application holds important data client-side in tokens (cookies, URLs, data files, and so forth) that data can be manipulated. If client or server-side application components...

- Using Alternative IP Address Encodings
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.0
  Risk Scores: Financial: 2.2800000000000002, Safety: 2.2800000000000002, Privacy: 9.120000000000001
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: This attack relies on the adversary using unexpected formats for representing IP addresses. Networked applications may expect network location information in a specific format, such as fully qualified...

- Exploiting Multiple Input Interpretation Layers
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.0
  Risk Scores: Financial: 2.2800000000000002, Safety: 2.2800000000000002, Privacy: 9.120000000000001
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: An attacker supplies the target software with input data that contains sequences of special characters designed to bypass input validation logic. This exploit relies on the target making multiples pas...

- Development Alteration
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.0
  Risk Scores: Financial: 2.2800000000000002, Safety: 2.2800000000000002, Privacy: 9.120000000000001
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: An adversary modifies a technology, product, or component during its development to acheive a negative impact once the system is deployed. The goal of the adversary is to modify the system in such a w...

- Malicious Logic Insertion into Product Software via Configuration Management Manipulation
  Impact Scores: Financial: 4.0, Safety: 1, Privacy: 1
  Risk Scores: Financial: 9.120000000000001, Safety: 2.2800000000000002, Privacy: 2.2800000000000002
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: An adversary exploits a configuration management system so that malicious logic is inserted into a software products build, update or deployed environment. If an adversary can control the elements inc...

- Design Alteration

Impact Scores: Financial: 1, Safety: 1, Privacy: 4.0
Risk Scores: Financial: 2.2800000000000002, Safety: 2.2800000000000002, Privacy: 9.120000000000001
Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
Description: An adversary modifies the design of a technology, product, or component to acheive a negative impact once the system is deployed. In this type of attack, the goal of the adversary is to modify the des...

- Contradictory Destinations in Traffic Routing Schemes
Impact Scores: Financial: 4.0, Safety: 1, Privacy: 1
Risk Scores: Financial: 9.120000000000001, Safety: 2.2800000000000002, Privacy: 2.2800000000000002
Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
Description: Adversaries can provide contradictory destinations when sending messages. Traffic is routed in networks using the domain names in various headers available at different levels of the OSI model. In a C...

- Object Injection
Impact Scores: Financial: 1, Safety: 1, Privacy: 4.0
Risk Scores: Financial: 2.2800000000000002, Safety: 2.2800000000000002, Privacy: 9.120000000000001
Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
Description: An adversary attempts to exploit an application by injecting additional, malicious content during its processing of serialized objects. Developers leverage serialization in order to convert data or st...

- Bluetooth Impersonation AttackS (BIAS)
Impact Scores: Financial: 4.0, Safety: 1, Privacy: 1
Risk Scores: Financial: 9.120000000000001, Safety: 2.2800000000000002, Privacy: 2.2800000000000002
Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
Description: An adversary disguises the MAC address of their Bluetooth enabled device to one for which there exists an active and trusted connection and authenticates successfully. The adversary can then perform m...

- Alteration of a Software Update
Impact Scores: Financial: 4.0, Safety: 1, Privacy: 1
Risk Scores: Financial: 9.120000000000001, Safety: 2.2800000000000002, Privacy: 2.2800000000000002
Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
Description: An adversary with access to an organization’s software update infrastructure inserts malware into the content of an outgoing update to fielded systems where a wide range of malicious effects are possi...

- Eavesdropping on a Monitor
Impact Scores: Financial: 1, Safety: 1, Privacy: 4.0
Risk Scores: Financial: 2.2800000000000002, Safety: 2.2800000000000002, Privacy: 9.120000000000001
Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
Description: An Adversary can eavesdrop on the content of an external monitor through the air without modifying any cable or installing software, just capturing this signal emitted by the cable or video port, with...

- Browser in the Middle (BiTM)
Impact Scores: Financial: 4.0, Safety: 1, Privacy: 1
Risk Scores: Financial: 9.120000000000001, Safety: 2.2800000000000002, Privacy: 2.2800000000000002
Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
Description: An adversary exploits the inherent functionalities of a web browser, in order to establish an unnoticed remote desktop connection in the victim's browser to the adversary's system. The adversary must ...

- Manipulating State
Impact Scores: Financial: 1, Safety: 1, Privacy: 4.0
Risk Scores: Financial: 2.2800000000000002, Safety: 2.2800000000000002, Privacy: 9.120000000000001
Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
Description: The adversary modifies state information maintained by the target software or causes a state transition in

hardware. If successful, the target will use this tainted state and execute in an unintended ...

- Escaping a Sandbox by Calling Code in Another Language
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5
  Risk Scores: Financial: 1.52, Safety: 1.52, Privacy: 7.6
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: The attacker may submit malicious code of another language to obtain access to privileges that were not intentionally exposed by the sandbox, thus escaping the sandbox. For instance, Java code cannot ...

- Hijacking a Privileged Thread of Execution
  Impact Scores: Financial: 5, Safety: 1, Privacy: 1
  Risk Scores: Financial: 7.6, Safety: 1.52, Privacy: 1.52
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: An adversary hijacks a privileged thread of execution by injecting malicious code into a running process. By using a privleged thread to do their bidding, adversaries can evade process-based detection...

- Subvert Code-signing Facilities
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5
  Risk Scores: Financial: 1.52, Safety: 1.52, Privacy: 7.6
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: Many languages use code signing facilities to vouch for code's identity and to thus tie code to its assigned privileges within an environment. Subverting this mechanism can be instrumental in an attac...

- Load Value Injection
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5
  Risk Scores: Financial: 1.52, Safety: 1.52, Privacy: 7.6
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: An adversary exploits a hardware design flaw in a CPU implementation of transient instruction execution in which a faulting or assisted load instruction transiently forwards adversary-controlled data ...

- Interface Manipulation
  Impact Scores: Financial: 3.0, Safety: 1, Privacy: 1
  Risk Scores: Financial: 6.840000000000001, Safety: 2.2800000000000002, Privacy: 2.2800000000000002
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: An adversary manipulates the use or processing of an interface (e.g. Application Programming Interface (API) or System-on-Chip (SoC)) resulting in an adverse impact upon the security of the system imp...

- Parameter Injection
  Impact Scores: Financial: 1, Safety: 1, Privacy: 3.0
  Risk Scores: Financial: 2.2800000000000002, Safety: 2.2800000000000002, Privacy: 6.840000000000001
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: An adversary manipulates the content of request parameters for the purpose of undermining the security of the target. Some parameter encodings use text characters as separators. For example, parameter...

- Content Spoofing
  Impact Scores: Financial: 3.0, Safety: 1, Privacy: 3.0
  Risk Scores: Financial: 6.840000000000001, Safety: 2.2800000000000002, Privacy: 6.840000000000001
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: An adversary modifies content to make it contain something other than what the original content producer intended while keeping the apparent source of the content unchanged. The term content spoofing ...

- Resource Location Spoofing
  Impact Scores: Financial: 1, Safety: 1, Privacy: 3.0

Risk Scores: Financial: 2.2800000000000002, Safety: 2.2800000000000002, Privacy: 6.840000000000001
Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
Description: An adversary deceives an application or user and convinces them to request a resource from an unintended location. By spoofing the location, the adversary can cause an alternate resource to be used, o...

- Cross-Site Flashing
  Impact Scores: Financial: 3.0, Safety: 1, Privacy: 1
  Risk Scores: Financial: 6.840000000000001, Safety: 2.2800000000000002, Privacy: 2.2800000000000002
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: An attacker is able to trick the victim into executing a Flash document that passes commands or calls to a Flash player browser plugin, allowing the attacker to exploit native Flash functionality in t...

- Modification of Registry Run Keys
  Impact Scores: Financial: 1, Safety: 1, Privacy: 3.0
  Risk Scores: Financial: 2.2800000000000002, Safety: 2.2800000000000002, Privacy: 6.840000000000001
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: An adversary adds a new entry to the run keys in the Windows registry so that an application of their choosing is executed when a user logs in. In this way, the adversary can get their executable to o...

- Using Leading 'Ghost' Character Sequences to Bypass Input Filters
  Impact Scores: Financial: 1, Safety: 1, Privacy: 3.0
  Risk Scores: Financial: 2.2800000000000002, Safety: 2.2800000000000002, Privacy: 6.840000000000001
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: Some APIs will strip certain leading characters from a string of parameters. An adversary can intentionally introduce leading ghost characters (extra characters that don't affect the validity of the r...

- Manipulate Human Behavior
  Impact Scores: Financial: 1, Safety: 1, Privacy: 3.0
  Risk Scores: Financial: 2.2800000000000002, Safety: 2.2800000000000002, Privacy: 6.840000000000001
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: An adversary exploits inherent human psychological predisposition to influence a targeted individual or group to solicit information or manipulate the target into performing an action that serves the ...

- Disable Security Software
  Impact Scores: Financial: 3.0, Safety: 1, Privacy: 1
  Risk Scores: Financial: 6.840000000000001, Safety: 2.2800000000000002, Privacy: 2.2800000000000002
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: An adversary exploits a weakness in access control to disable security tools so that detection does not occur. This can take the form of killing processes, deleting registry keys so that tools do not ...

- Collect Data from Registries
  Impact Scores: Financial: 1, Safety: 1, Privacy: 3.0
  Risk Scores: Financial: 2.2800000000000002, Safety: 2.2800000000000002, Privacy: 6.840000000000001
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: An adversary exploits a weakness in authorization to gather system-specific data and sensitive information within a registry (e.g., Windows Registry, Mac plist). These contain information about the sy...

- Collect Data from Screen Capture
  Impact Scores: Financial: 1, Safety: 1, Privacy: 3.0
  Risk Scores: Financial: 2.2800000000000002, Safety: 2.2800000000000002, Privacy: 6.840000000000001
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: An adversary gathers sensitive information by exploiting the system's screen capture functionality. Through screenshots, the adversary aims to see what happens on the screen over the course of an oper...

- Retrieve Data from Decommissioned Devices
  Impact Scores: Financial: 1, Safety: 1, Privacy: 3.0
  Risk Scores: Financial: 2.2800000000000002, Safety: 2.2800000000000002, Privacy: 6.840000000000001
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: An adversary obtains decommissioned, recycled, or discarded systems and devices that can include an organization’s intellectual property, employee data, and other types of controlled information. Syst...

- Web Application Fingerprinting
  Impact Scores: Financial: 1, Safety: 1, Privacy: 2.0
  Risk Scores: Financial: 3.04, Safety: 3.04, Privacy: 6.08
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: An attacker sends a series of probes to a web application in order to elicit version-dependent and type-dependent behavior that assists in identifying the target. An attacker could learn information s...

- Fuzzing for application mapping
  Impact Scores: Financial: 1, Safety: 2.0, Privacy: 1
  Risk Scores: Financial: 3.04, Safety: 6.08, Privacy: 3.04
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: An attacker sends random, malformed, or otherwise unexpected messages to a target application and observes the application's log or error messages returned. The attacker does not initially know how a ...

- Forced Deadlock
  Impact Scores: Financial: 4.0, Safety: 1, Privacy: 1
  Risk Scores: Financial: 6.08, Safety: 1.52, Privacy: 1.52
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: The adversary triggers and exploits a deadlock condition in the target software to cause a denial of service. A deadlock can occur when two or more competing actions are waiting for each other to fini...

- Schema Poisoning
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.0
  Risk Scores: Financial: 1.52, Safety: 1.52, Privacy: 6.08
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: An adversary corrupts or modifies the content of a schema for the purpose of undermining the security of the target. Schemas provide the structure and content definitions for resources used by an appl...

- USB Memory Attacks
  Impact Scores: Financial: 2.0, Safety: 1, Privacy: 4.0
  Risk Scores: Financial: 3.04, Safety: 1.52, Privacy: 6.08
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: An adversary loads malicious code onto a USB memory stick in order to infect any system which the device is plugged in to. USB drives present a significant security risk for business and government ag...

- Signature Spoofing by Misrepresentation
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.0
  Risk Scores: Financial: 1.52, Safety: 1.52, Privacy: 6.08
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: An attacker exploits a weakness in the parsing or display code of the recipient software to generate a data blob containing a supposedly valid signature, but the signer's identity is falsely represent...

- Hardware Component Substitution During Baselining
  Impact Scores: Financial: 4.0, Safety: 1, Privacy: 1
  Risk Scores: Financial: 6.08, Safety: 1.52, Privacy: 1.52
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20

Description: An adversary with access to system components during allocated baseline development can substitute a maliciously altered hardware component for a baseline component during the product development and ...

- Malicious Hardware Update
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.0
  Risk Scores: Financial: 1.52, Safety: 1.52, Privacy: 6.08
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: An adversary introduces malicious hardware during an update or replacement procedure, allowing for additional compromise or site disruption at the victim location. After deployment, it is not uncommon...

- Open-Source Library Manipulation
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.0
  Risk Scores: Financial: 1.52, Safety: 1.52, Privacy: 6.08
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: Adversaries implant malicious code in open source software (OSS) libraries to have it widely distributed, as OSS is commonly downloaded by developers and other users to incorporate into software devel...

- ASIC With Malicious Functionality
  Impact Scores: Financial: 4.0, Safety: 1, Privacy: 1
  Risk Scores: Financial: 6.08, Safety: 1.52, Privacy: 1.52
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: An attacker with access to the development environment process of an application-specific integrated circuit (ASIC) for a victim system being developed or maintained after initial deployment can inser...

- Hardware Fault Injection
  Impact Scores: Financial: 1, Safety: 4.0, Privacy: 4.0
  Risk Scores: Financial: 1.52, Safety: 6.08, Privacy: 6.08
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: The adversary uses disruptive signals or events, or alters the physical environment a device operates in, to cause faulty behavior in electronic devices. This can include electromagnetic pulses, laser...

- Carry-Off GPS Attack
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.0
  Risk Scores: Financial: 1.52, Safety: 1.52, Privacy: 6.08
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: A common form of a GPS spoofing attack, commonly termed a carry-off attack begins with an adversary broadcasting signals synchronized with the genuine signals observed by the target receiver. The powe...

- DLL Side-Loading
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.0
  Risk Scores: Financial: 1.52, Safety: 1.52, Privacy: 6.08
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: An adversary places a malicious version of a Dynamic-Link Library (DLL) in the Windows Side-by-Side (WinSxS) directory to trick the operating system into loading this malicious DLL instead of a legiti...

- Use of Captured Tickets (Pass The Ticket)
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.0
  Risk Scores: Financial: 1.52, Safety: 1.52, Privacy: 6.08
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: An adversary uses stolen Kerberos tickets to access systems/resources that leverage the Kerberos authentication protocol. The Kerberos authentication protocol centers around a ticketing system which i...

- Sniff Application Code

Impact Scores: Financial: 1, Safety: 1, Privacy: 4.0
Risk Scores: Financial: 1.52, Safety: 1.52, Privacy: 6.08
Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
Description: An adversary passively sniffs network communications and captures application code bound for an authorized client. Once obtained, they can use it as-is, or through reverse-engineering glean sensitive ...

- Key Negotiation of Bluetooth Attack (KNOB)
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.0
  Risk Scores: Financial: 1.52, Safety: 1.52, Privacy: 6.08
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: An adversary can exploit a flaw in Bluetooth key negotiation allowing them to decrypt information sent between two devices communicating via Bluetooth. The adversary uses an Adversary in the Middle se...

- Malicious Code Implanted During Chip Programming
  Impact Scores: Financial: 4.0, Safety: 1, Privacy: 1
  Risk Scores: Financial: 6.08, Safety: 1.52, Privacy: 1.52
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: During the programming step of chip manufacture, an adversary with access and necessary technical skills maliciously alters a chip’s intended program logic to produce an effect intended by the adversa...

- AJAX Footprinting
  Impact Scores: Financial: 1, Safety: 1, Privacy: 2.0
  Risk Scores: Financial: 3.04, Safety: 3.04, Privacy: 6.08
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: This attack utilizes the frequent client-server roundtrips in Ajax conversation to scan a system. While Ajax does not open up new vulnerabilities per se, it does optimize them from an attacker point o...

- Interception
  Impact Scores: Financial: 1, Safety: 1, Privacy: 3.0
  Risk Scores: Financial: 1.52, Safety: 1.52, Privacy: 4.5600000000000005
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: An adversary monitors data streams to or from the target for information gathering purposes. This attack may be undertaken to solely gather sensitive information or to support a further attack against...

- XML Ping of the Death
  Impact Scores: Financial: 1, Safety: 3.0, Privacy: 1
  Risk Scores: Financial: 1.52, Safety: 4.5600000000000005, Privacy: 1.52
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: An attacker initiates a resource depletion attack where a large number of small XML messages are delivered at a sufficiently rapid rate to cause a denial of service or crash of the target. Transaction...

- Active OS Fingerprinting
  Impact Scores: Financial: 1, Safety: 1, Privacy: 2.0
  Risk Scores: Financial: 2.2800000000000002, Safety: 2.2800000000000002, Privacy: 4.5600000000000005
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: An adversary engages in activity to detect the operating system or firmware version of a remote target by interrogating a device, server, or platform with a probe designed to solicit behavior that wil...

- TCP Timestamp Probe
  Impact Scores: Financial: 2.0, Safety: 1, Privacy: 1
  Risk Scores: Financial: 4.5600000000000005, Safety: 2.2800000000000002, Privacy: 2.2800000000000002
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: This OS fingerprinting probe examines the remote server's implementation of TCP timestamps. Not all

operating systems implement timestamps within the TCP header, but when timestamps are used then this...

- TCP Sequence Number Probe
  Impact Scores: Financial: 2.0, Safety: 1, Privacy: 1
  Risk Scores: Financial: 4.5600000000000005, Safety: 2.2800000000000002, Privacy: 2.2800000000000002
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: This OS fingerprinting probe tests the target system's assignment of TCP sequence numbers. One common way to test TCP Sequence Number generation is to send a probe packet to an open port on the target...

- TCP (ISN) Greatest Common Divisor Probe
  Impact Scores: Financial: 1, Safety: 1, Privacy: 2.0
  Risk Scores: Financial: 2.2800000000000002, Safety: 2.2800000000000002, Privacy: 4.5600000000000005
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: This OS fingerprinting probe sends a number of TCP SYN packets to an open port of a remote machine. The Initial Sequence Number (ISN) in each of the SYN/ACK response packets is analyzed to determine t...

- TCP (ISN) Counter Rate Probe
  Impact Scores: Financial: 1, Safety: 1, Privacy: 2.0
  Risk Scores: Financial: 2.2800000000000002, Safety: 2.2800000000000002, Privacy: 4.5600000000000005
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: This OS detection probe measures the average rate of initial sequence number increments during a period of time. Sequence numbers are incremented using a time-based algorithm and are susceptible to a ...

- TCP (ISN) Sequence Predictability Probe
  Impact Scores: Financial: 1, Safety: 1, Privacy: 2.0
  Risk Scores: Financial: 2.2800000000000002, Safety: 2.2800000000000002, Privacy: 4.5600000000000005
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: This type of operating system probe attempts to determine an estimate for how predictable the sequence number generation algorithm is for a remote host. Statistical techniques, such as standard deviat...

- TCP Initial Window Size Probe
  Impact Scores: Financial: 2.0, Safety: 1, Privacy: 1
  Risk Scores: Financial: 4.5600000000000005, Safety: 2.2800000000000002, Privacy: 2.2800000000000002
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: This OS fingerprinting probe checks the initial TCP Window size. TCP stacks limit the range of sequence numbers allowable within a session to maintain the connected state within TCP protocol logic. Th...

- TCP Options Probe
  Impact Scores: Financial: 2.0, Safety: 1, Privacy: 1
  Risk Scores: Financial: 4.5600000000000005, Safety: 2.2800000000000002, Privacy: 2.2800000000000002
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: This OS fingerprinting probe analyzes the type and order of any TCP header options present within a response segment. Most operating systems use unique ordering and different option sets when options ...

- Pretexting
  Impact Scores: Financial: 1, Safety: 1, Privacy: 2.0
  Risk Scores: Financial: 2.2800000000000002, Safety: 2.2800000000000002, Privacy: 4.5600000000000005
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: An adversary engages in pretexting behavior to solicit information from target persons, or manipulate the target into performing some action that serves the adversary's interests. During a pretexting ...

- Incomplete Data Deletion in a Multi-Tenant Environment
  Impact Scores: Financial: 1, Safety: 1, Privacy: 3.0

Risk Scores: Financial: 1.52, Safety: 1.52, Privacy: 4.5600000000000005
Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
Description: An adversary obtains unauthorized information due to insecure or incomplete data deletion in a multi-tenant environment. If a cloud provider fails to completely delete storage and data from former clo...

- Adding a Space to a File Extension
Impact Scores: Financial: 1, Safety: 1, Privacy: 3.0
Risk Scores: Financial: 1.52, Safety: 1.52, Privacy: 4.5600000000000005
Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
Description: An adversary adds a space character to the end of a file extension and takes advantage of an application that does not properly neutralize trailing special elements in file names. This extra space, wh...

- Reverse Engineering
Impact Scores: Financial: 2.0, Safety: 1, Privacy: 1
Risk Scores: Financial: 3.04, Safety: 1.52, Privacy: 1.52
Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
Description: An adversary discovers the structure, function, and composition of an object, resource, or system by using a variety of analysis techniques to effectively determine how the analyzed entity was constru...

- Fingerprinting
Impact Scores: Financial: 1, Safety: 1, Privacy: 1
Risk Scores: Financial: 3.04, Safety: 3.04, Privacy: 3.04
Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
Description: An adversary compares output from a target system to known indicators that uniquely identify specific details about the target. Most commonly, fingerprinting is done to determine operating system and ...

- Target Influence via Framing
Impact Scores: Financial: 1, Safety: 1, Privacy: 2.0
Risk Scores: Financial: 1.52, Safety: 1.52, Privacy: 3.04
Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
Description: An adversary uses framing techniques to contextualize a conversation so that the target is more likely to be influenced by the adversary's point of view. Framing is information and experiences in life...

- Influence via Psychological Principles
Impact Scores: Financial: 2.0, Safety: 1, Privacy: 1
Risk Scores: Financial: 3.04, Safety: 1.52, Privacy: 1.52
Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
Description: The adversary shapes the target's actions or behavior by focusing on the ways human interact and learn, leveraging such elements as cognitive and social psychology. In a variety of ways, a target can ...

- Process Footprinting
Impact Scores: Financial: 1, Safety: 1, Privacy: 2.0
Risk Scores: Financial: 1.52, Safety: 1.52, Privacy: 3.04
Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
Description: An adversary exploits functionality meant to identify information about the currently running processes on the target system to an authorized user. By knowing what processes are running on the target ...

- Services Footprinting
Impact Scores: Financial: 1, Safety: 1, Privacy: 2.0
Risk Scores: Financial: 1.52, Safety: 1.52, Privacy: 3.04
Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
Description: An adversary exploits functionality meant to identify information about the services on the target system to an authorized user. By knowing what services are registered on the target system, the adver...

- Account Footprinting
  Impact Scores: Financial: 1, Safety: 1, Privacy: 2.0
  Risk Scores: Financial: 1.52, Safety: 1.52, Privacy: 3.04
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: An adversary exploits functionality meant to identify information about the domain accounts and their permissions on the target system to an authorized user. By knowing what accounts are registered on...

- Group Permission Footprinting
  Impact Scores: Financial: 1, Safety: 1, Privacy: 2.0
  Risk Scores: Financial: 1.52, Safety: 1.52, Privacy: 3.04
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: An adversary exploits functionality meant to identify information about user groups and their permissions on the target system to an authorized user. By knowing what users/permissions are registered o...

- Owner Footprinting
  Impact Scores: Financial: 1, Safety: 1, Privacy: 2.0
  Risk Scores: Financial: 1.52, Safety: 1.52, Privacy: 3.04
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: An adversary exploits functionality meant to identify information about the primary users on the target system to an authorized user. They may do this, for example, by reviewing logins or file modific...

- System Footprinting
  Impact Scores: Financial: 1, Safety: 1, Privacy: 2.0
  Risk Scores: Financial: 1.52, Safety: 1.52, Privacy: 3.04
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: An adversary engages in active probing and exploration activities to determine security information about a remote target system. Often times adversaries will rely on remote applications that can be p...

- Collect Data from Clipboard
  Impact Scores: Financial: 1, Safety: 1, Privacy: 2.0
  Risk Scores: Financial: 1.52, Safety: 1.52, Privacy: 3.04
  Risk Factors: exposure: 1.00, complexity: 0.30, attack_surface: 0.20
  Description: The adversary exploits an application that allows for the copying of sensitive data or information by collecting information copied to the clipboard. Data copied to the clipboard can be accessed by ot...

Component: Telematics Gateway

Type: Gateway
Safety Level: ASIL C
Interfaces: CAN, 4G, Ethernet
Access Points: Debug Port, USB
Data Types: Diagnostic Data, All Traffic, Telemetry
Location: Internal
Trust Zone: Boundary
Connected To: ECU003, ECU001, ECU002

Identified Threats:

- Buffer Manipulation
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5
  Risk Scores: Financial: 3.5199999999999996, Safety: 3.5199999999999996, Privacy: 17.599999999999998

Risk Factors: exposure: 0.70, complexity: 0.90, attack_surface: 1.00
Description: An adversary manipulates an application's interaction with a buffer in an attempt to read or modify data they shouldn't have access to. Buffer attacks are distinguished in that it is the buffer space ...

- Redirect Access to Libraries
Impact Scores: Financial: 1, Safety: 5, Privacy: 1
Risk Scores: Financial: 3.5199999999999996, Safety: 17.599999999999998, Privacy: 3.5199999999999996
Risk Factors: exposure: 0.70, complexity: 0.90, attack_surface: 1.00
Description: An adversary exploits a weakness in the way an application searches for external libraries to manipulate the execution flow to point to an adversary supplied library or code base. This pattern of atta...

- XSS Targeting Non-Script Elements
Impact Scores: Financial: 1, Safety: 1, Privacy: 5
Risk Scores: Financial: 3.5199999999999996, Safety: 3.5199999999999996, Privacy: 17.599999999999998
Risk Factors: exposure: 0.70, complexity: 0.90, attack_surface: 1.00
Description: This attack is a form of Cross-Site Scripting (XSS) where malicious scripts are embedded in elements that are not expected to host scripts such as image tags (<img>), comments in XML documents (< !-CD...

- Retrieve Embedded Sensitive Data
Impact Scores: Financial: 1, Safety: 1, Privacy: 5
Risk Scores: Financial: 3.5199999999999996, Safety: 3.5199999999999996, Privacy: 17.599999999999998
Risk Factors: exposure: 0.70, complexity: 0.90, attack_surface: 1.00
Description: An attacker examines a target system to find sensitive data that has been embedded within it. This information can reveal confidential contents, such as account numbers or individual keys/credentials ...

- Leveraging/Manipulating Configuration File Search Paths
Impact Scores: Financial: 5, Safety: 1, Privacy: 1
Risk Scores: Financial: 17.599999999999998, Safety: 3.5199999999999996, Privacy: 3.5199999999999996
Risk Factors: exposure: 0.70, complexity: 0.90, attack_surface: 1.00
Description: This pattern of attack sees an adversary load a malicious resource into a program's standard path so that when a known command is executed then the system instead executes the malicious component. The...

- Manipulating Writeable Terminal Devices
Impact Scores: Financial: 1, Safety: 1, Privacy: 5
Risk Scores: Financial: 3.5199999999999996, Safety: 3.5199999999999996, Privacy: 17.599999999999998
Risk Factors: exposure: 0.70, complexity: 0.90, attack_surface: 1.00
Description: This attack exploits terminal devices that allow themselves to be written to by other users. The attacker sends command strings to the target terminal device hoping that the target user will hit enter...

- Overflow Binary Resource File
Impact Scores: Financial: 5, Safety: 1, Privacy: 1
Risk Scores: Financial: 17.599999999999998, Safety: 3.5199999999999996, Privacy: 3.5199999999999996
Risk Factors: exposure: 0.70, complexity: 0.90, attack_surface: 1.00
Description: An attack of this type exploits a buffer overflow vulnerability in the handling of binary resources. Binary resources may include music files like MP3, image files like JPEG files, and any other binar...

- Poison Web Service Registry
Impact Scores: Financial: 1, Safety: 1, Privacy: 5
Risk Scores: Financial: 3.5199999999999996, Safety: 3.5199999999999996, Privacy: 17.599999999999998
Risk Factors: exposure: 0.70, complexity: 0.90, attack_surface: 1.00
Description: SOA and Web Services often use a registry to perform look up, get schema information, and metadata about services. A poisoned registry can redirect (think phishing for servers) the service requester t...

- String Format Overflow in syslog()
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5
  Risk Scores: Financial: 3.5199999999999996, Safety: 3.5199999999999996, Privacy: 17.599999999999998
  Risk Factors: exposure: 0.70, complexity: 0.90, attack_surface: 1.00
  Description: This attack targets applications and software that uses the syslog() function insecurely. If an application does not explicitely use a format string parameter in a call to syslog(), user input can be ...

- Manipulating User-Controlled Variables
  Impact Scores: Financial: 2.4, Safety: 1, Privacy: 5
  Risk Scores: Financial: 8.447999999999999, Safety: 3.5199999999999996, Privacy: 17.599999999999998
  Risk Factors: exposure: 0.70, complexity: 0.90, attack_surface: 1.00
  Description: This attack targets user controlled variables (DEBUG=1, PHP Globals, and So Forth). An adversary can override variables leveraging user-supplied, untrusted query variables directly used on the applica...

- XQuery Injection
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5
  Risk Scores: Financial: 3.5199999999999996, Safety: 3.5199999999999996, Privacy: 17.599999999999998
  Risk Factors: exposure: 0.70, complexity: 0.90, attack_surface: 1.00
  Description: This attack utilizes XQuery to probe and attack server systems; in a similar manner that SQL Injection allows an attacker to exploit SQL calls to RDBMS, XQuery Injection uses improperly validated data...

- Pharming
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5
  Risk Scores: Financial: 3.5199999999999996, Safety: 3.5199999999999996, Privacy: 17.599999999999998
  Risk Factors: exposure: 0.70, complexity: 0.90, attack_surface: 1.00
  Description: A pharming attack occurs when the victim is fooled into entering sensitive data into supposedly trusted locations, such as an online bank site or a trading platform. An attacker can impersonate these ...

- Phishing
  Impact Scores: Financial: 1.2, Safety: 1, Privacy: 5
  Risk Scores: Financial: 4.223999999999999, Safety: 3.5199999999999996, Privacy: 17.599999999999998
  Risk Factors: exposure: 0.70, complexity: 0.90, attack_surface: 1.00
  Description: Phishing is a social engineering technique where an attacker masquerades as a legitimate entity with which the victim might do business in order to prompt the user to reveal some confidential informat...

- Accessing Functionality Not Properly Constrained by ACLs
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.8
  Risk Scores: Financial: 3.5199999999999996, Safety: 3.5199999999999996, Privacy: 16.895999999999997
  Risk Factors: exposure: 0.70, complexity: 0.90, attack_surface: 1.00
  Description: In applications, particularly web applications, access to functionality is mitigated by an authorization framework. This framework maps Access Control Lists (ACLs) to elements of the application's fun...

- Buffer Overflow via Environment Variables
  Impact Scores: Financial: 4.8, Safety: 1, Privacy: 1
  Risk Scores: Financial: 16.895999999999997, Safety: 3.5199999999999996, Privacy: 3.5199999999999996
  Risk Factors: exposure: 0.70, complexity: 0.90, attack_surface: 1.00
  Description: This attack pattern involves causing a buffer overflow through manipulation of environment variables. Once the adversary finds that they can modify an environment variable, they may try to overflow as...

- Server Side Include (SSI) Injection
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.8
  Risk Scores: Financial: 3.5199999999999996, Safety: 3.5199999999999996, Privacy: 16.895999999999997
  Risk Factors: exposure: 0.70, complexity: 0.90, attack_surface: 1.00

Description: An attacker can use Server Side Include (SSI) Injection to send code to a web application that then gets executed by the web server. Doing so enables the attacker to achieve similar results to Cross S...

- Format String Injection
  Impact Scores: Financial: 1, Safety: 2.4, Privacy: 4.8
  Risk Scores: Financial: 3.5199999999999996, Safety: 8.447999999999999, Privacy: 16.895999999999997
  Risk Factors: exposure: 0.70, complexity: 0.90, attack_surface: 1.00
  Description: An adversary includes formatting characters in a string input field on the target application. Most applications assume that users will provide static text and may respond unpredictably to the presenc...

- Cache Poisoning
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.8
  Risk Scores: Financial: 3.5199999999999996, Safety: 3.5199999999999996, Privacy: 16.895999999999997
  Risk Factors: exposure: 0.70, complexity: 0.90, attack_surface: 1.00
  Description: An attacker exploits the functionality of cache technologies to cause specific data to be cached that aids the attackers' objectives. This describes any attack whereby an attacker places incorrect or ...

- DNS Cache Poisoning
  Impact Scores: Financial: 4.8, Safety: 1, Privacy: 1
  Risk Scores: Financial: 16.895999999999997, Safety: 3.5199999999999996, Privacy: 3.5199999999999996
  Risk Factors: exposure: 0.70, complexity: 0.90, attack_surface: 1.00
  Description: A domain name server translates a domain name (such as www.example.com) into an IP address that Internet hosts use to contact Internet resources. An adversary modifies a public DNS cache to cause cert...

- Command Delimiters
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.8
  Risk Scores: Financial: 3.5199999999999996, Safety: 3.5199999999999996, Privacy: 16.895999999999997
  Risk Factors: exposure: 0.70, complexity: 0.90, attack_surface: 1.00
  Description: An attack of this type exploits a programs' vulnerabilities that allows an attacker's commands to be concatenated onto a legitimate command with the intent of targeting other resources such as the fil...

- Malicious Automated Software Update via Redirection
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.8
  Risk Scores: Financial: 3.5199999999999996, Safety: 3.5199999999999996, Privacy: 16.895999999999997
  Risk Factors: exposure: 0.70, complexity: 0.90, attack_surface: 1.00
  Description: An attacker exploits two layers of weaknesses in server or client software for automated update mechanisms to undermine the integrity of the target code-base. The first weakness involves a failure to ...

- PHP Remote File Inclusion
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.8
  Risk Scores: Financial: 3.5199999999999996, Safety: 3.5199999999999996, Privacy: 16.895999999999997
  Risk Factors: exposure: 0.70, complexity: 0.90, attack_surface: 1.00
  Description: In this pattern the adversary is able to load and execute arbitrary code remotely available from the application. This is usually accomplished through an insecurely configured PHP runtime environment ...

- XSS Using Alternate Syntax
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.8
  Risk Scores: Financial: 3.5199999999999996, Safety: 3.5199999999999996, Privacy: 16.895999999999997
  Risk Factors: exposure: 0.70, complexity: 0.90, attack_surface: 1.00
  Description: An adversary uses alternate forms of keywords or commands that result in the same action as the primary form but which may not be caught by filters. For example, many keywords are processed in a case ...

- Serialized Data External Linking

Impact Scores: Financial: 1, Safety: 1, Privacy: 4.8
Risk Scores: Financial: 3.5199999999999996, Safety: 3.5199999999999996, Privacy: 16.895999999999997
Risk Factors: exposure: 0.70, complexity: 0.90, attack_surface: 1.00
Description: An adversary creates a serialized data file (e.g. XML, YAML, etc...) that contains an external data reference. Because serialized data parsers may not validate documents with external references, ther...

- Leveraging Race Conditions
Impact Scores: Financial: 4.8, Safety: 1, Privacy: 1
Risk Scores: Financial: 16.895999999999997, Safety: 3.5199999999999996, Privacy: 3.5199999999999996
Risk Factors: exposure: 0.70, complexity: 0.90, attack_surface: 1.00
Description: The adversary targets a race condition occurring when multiple processes access and manipulate the same resource concurrently, and the outcome of the execution depends on the particular order in which...

- Leveraging Time-of-Check and Time-of-Use (TOCTOU) Race Conditions
Impact Scores: Financial: 4.8, Safety: 1, Privacy: 1
Risk Scores: Financial: 16.895999999999997, Safety: 3.5199999999999996, Privacy: 3.5199999999999996
Risk Factors: exposure: 0.70, complexity: 0.90, attack_surface: 1.00
Description: This attack targets a race condition occurring between the time of check (state) for a resource and the time of use of a resource. A typical example is file access. The adversary can leverage a file a...

- Using Meta-characters in E-mail Headers to Inject Malicious Payloads
Impact Scores: Financial: 1, Safety: 1, Privacy: 4.8
Risk Scores: Financial: 3.5199999999999996, Safety: 3.5199999999999996, Privacy: 16.895999999999997
Risk Factors: exposure: 0.70, complexity: 0.90, attack_surface: 1.00
Description: This type of attack involves an attacker leveraging meta-characters in email headers to inject improper behavior into email programs. Email software has become increasingly sophisticated and feature-r...

- Buffer Overflow via Symbolic Links
Impact Scores: Financial: 1, Safety: 1, Privacy: 4.8
Risk Scores: Financial: 3.5199999999999996, Safety: 3.5199999999999996, Privacy: 16.895999999999997
Risk Factors: exposure: 0.70, complexity: 0.90, attack_surface: 1.00
Description: This type of attack leverages the use of symbolic links to cause buffer overflows. An adversary can try to create or manipulate a symbolic link file such that its contents result in out of bounds data...

- Passing Local Filenames to Functions That Expect a URL
Impact Scores: Financial: 1, Safety: 1, Privacy: 4.8
Risk Scores: Financial: 3.5199999999999996, Safety: 3.5199999999999996, Privacy: 16.895999999999997
Risk Factors: exposure: 0.70, complexity: 0.90, attack_surface: 1.00
Description: This attack relies on client side code to access local files and resources instead of URLs. When the client browser is expecting a URL string, but instead receives a request for a local file, that exe...

- Session Credential Falsification through Prediction
Impact Scores: Financial: 4.8, Safety: 1, Privacy: 1
Risk Scores: Financial: 16.895999999999997, Safety: 3.5199999999999996, Privacy: 3.5199999999999996
Risk Factors: exposure: 0.70, complexity: 0.90, attack_surface: 1.00
Description: This attack targets predictable session ID in order to gain privileges. The attacker can predict the session ID used during a transaction to perform spoofing and session hijacking....

- Using Slashes and URL Encoding Combined to Bypass Validation Logic
Impact Scores: Financial: 4.8, Safety: 1, Privacy: 1
Risk Scores: Financial: 16.895999999999997, Safety: 3.5199999999999996, Privacy: 3.5199999999999996
Risk Factors: exposure: 0.70, complexity: 0.90, attack_surface: 1.00
Description: This attack targets the encoding of the URL combined with the encoding of the slash characters. An

attacker can take advantage of the multiple ways of encoding a URL and abuse the interpretation of th...

- Voice Phishing
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.8
  Risk Scores: Financial: 3.5199999999999996, Safety: 3.5199999999999996, Privacy: 16.895999999999997
  Risk Factors: exposure: 0.70, complexity: 0.90, attack_surface: 1.00
  Description: An adversary targets users with a phishing attack for the purpose of soliciting account passwords or sensitive information from the user. Voice Phishing is a variation of the Phishing social engineeri...

- Malicious Automated Software Update via Spoofing
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.8
  Risk Scores: Financial: 3.5199999999999996, Safety: 3.5199999999999996, Privacy: 16.895999999999997
  Risk Factors: exposure: 0.70, complexity: 0.90, attack_surface: 1.00
  Description: An attackers uses identify or content spoofing to trick a client into performing an automated software update from a malicious source. A malicious automated software update that leverages spoofing can...

- Blind SQL Injection
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.8
  Risk Scores: Financial: 3.5199999999999996, Safety: 3.5199999999999996, Privacy: 16.895999999999997
  Risk Factors: exposure: 0.70, complexity: 0.90, attack_surface: 1.00
  Description: Blind SQL Injection results from an insufficient mitigation for SQL Injection. Although suppressing database error messages are considered best practice, the suppression alone is not sufficient to pre...

- URL Encoding
  Impact Scores: Financial: 4.8, Safety: 1, Privacy: 1
  Risk Scores: Financial: 16.895999999999997, Safety: 3.5199999999999996, Privacy: 3.5199999999999996
  Risk Factors: exposure: 0.70, complexity: 0.90, attack_surface: 1.00
  Description: This attack targets the encoding of the URL. An adversary can take advantage of the multiple way of encoding an URL and abuse the interpretation of the URL....

- User-Controlled Filename
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.8
  Risk Scores: Financial: 3.5199999999999996, Safety: 3.5199999999999996, Privacy: 16.895999999999997
  Risk Factors: exposure: 0.70, complexity: 0.90, attack_surface: 1.00
  Description: An attack of this type involves an adversary inserting malicious characters (such as a XSS redirection) into a filename, directly or indirectly that is then used by the target software to generate HTM...

- Using Escaped Slashes in Alternate Encoding
  Impact Scores: Financial: 4.8, Safety: 1, Privacy: 1
  Risk Scores: Financial: 16.895999999999997, Safety: 3.5199999999999996, Privacy: 3.5199999999999996
  Risk Factors: exposure: 0.70, complexity: 0.90, attack_surface: 1.00
  Description: This attack targets the use of the backslash in alternate encoding. An adversary can provide a backslash as a leading character and causes a parser to believe that the next character is special. This ...

- Buffer Overflow in an API Call
  Impact Scores: Financial: 4.8, Safety: 1, Privacy: 1
  Risk Scores: Financial: 16.895999999999997, Safety: 3.5199999999999996, Privacy: 3.5199999999999996
  Risk Factors: exposure: 0.70, complexity: 0.90, attack_surface: 1.00
  Description: This attack targets libraries or shared code modules which are vulnerable to buffer overflow attacks. An adversary who has knowledge of known vulnerable libraries or shared code can easily target soft...

- Using UTF-8 Encoding to Bypass Validation Logic
  Impact Scores: Financial: 1, Safety: 4.8, Privacy: 1

Risk Scores: Financial: 3.5199999999999996, Safety: 16.895999999999997, Privacy: 3.5199999999999996
Risk Factors: exposure: 0.70, complexity: 0.90, attack_surface: 1.00
Description: This attack is a specific variation on leveraging alternate encodings to bypass validation logic. This attack leverages the possibility to encode potentially harmful input in UTF-8 and submit it to ap...

- XPath Injection
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.8
  Risk Scores: Financial: 3.5199999999999996, Safety: 3.5199999999999996, Privacy: 16.895999999999997
  Risk Factors: exposure: 0.70, complexity: 0.90, attack_surface: 1.00
  Description: An attacker can craft special user-controllable input consisting of XPath expressions to inject the XML database and bypass authentication or glean information that they normally would not be able to....

- OS Command Injection
  Impact Scores: Financial: 4.8, Safety: 1, Privacy: 1
  Risk Scores: Financial: 16.895999999999997, Safety: 3.5199999999999996, Privacy: 3.5199999999999996
  Risk Factors: exposure: 0.70, complexity: 0.90, attack_surface: 1.00
  Description: In this type of an attack, an adversary injects operating system commands into existing application functions. An application that uses untrusted input to build command strings is vulnerable. An adver...

- Buffer Overflow in Local Command-Line Utilities
  Impact Scores: Financial: 4.8, Safety: 1, Privacy: 1
  Risk Scores: Financial: 16.895999999999997, Safety: 3.5199999999999996, Privacy: 3.5199999999999996
  Risk Factors: exposure: 0.70, complexity: 0.90, attack_surface: 1.00
  Description: This attack targets command-line utilities available in a number of shells. An adversary can leverage a vulnerability found in a command-line utility to escalate privilege to root....

- Reflection Attack in Authentication Protocol
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.8
  Risk Scores: Financial: 3.5199999999999996, Safety: 3.5199999999999996, Privacy: 16.895999999999997
  Risk Factors: exposure: 0.70, complexity: 0.90, attack_surface: 1.00
  Description: An adversary can abuse an authentication protocol susceptible to reflection attack in order to defeat it. Doing so allows the adversary illegitimate access to the target system, without possessing the...

- Forced Integer Overflow
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.8
  Risk Scores: Financial: 3.5199999999999996, Safety: 3.5199999999999996, Privacy: 16.895999999999997
  Risk Factors: exposure: 0.70, complexity: 0.90, attack_surface: 1.00
  Description: This attack forces an integer variable to go out of range. The integer variable is often used as an offset such as size of memory allocation or similarly. The attacker would typically control the valu...

- WSDL Scanning
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.8
  Risk Scores: Financial: 3.5199999999999996, Safety: 3.5199999999999996, Privacy: 16.895999999999997
  Risk Factors: exposure: 0.70, complexity: 0.90, attack_surface: 1.00
  Description: This attack targets the WSDL interface made available by a web service. The attacker may scan the WSDL interface to reveal sensitive information about invocation patterns, underlying technology implem...

- Gateway Compromise
  Impact Scores: Financial: 4.8, Safety: 4.8, Privacy: 5
  Risk Scores: Financial: 12.671999999999999, Safety: 12.671999999999999, Privacy: 13.2
  Risk Factors: exposure: 0.70, complexity: 0.90, attack_surface: 1.00
  Description: Compromise of network gateway leading to unauthorized network access...

- Root/Jailbreak Detection Evasion via Debugging
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5
  Risk Scores: Financial: 2.6399999999999997, Safety: 2.6399999999999997, Privacy: 13.2
  Risk Factors: exposure: 0.70, complexity: 0.90, attack_surface: 1.00
  Description: An adversary inserts a debugger into the program entry point of a mobile application to modify the application binary, with the goal of evading Root/Jailbreak detection. Mobile device users often Root...

- CAN Injection
  Impact Scores: Financial: 3.5999999999999996, Safety: 4.8, Privacy: 2.4
  Risk Scores: Financial: 9.503999999999998, Safety: 12.671999999999999, Privacy: 6.335999999999999
  Risk Factors: exposure: 0.70, complexity: 0.90, attack_surface: 1.00
  Description: Manipulation of CAN bus messages leading to vehicle malfunction...

- HTTP Request Splitting
  Impact Scores: Financial: 4.8, Safety: 1, Privacy: 1
  Risk Scores: Financial: 12.671999999999999, Safety: 2.6399999999999997, Privacy: 2.6399999999999997
  Risk Factors: exposure: 0.70, complexity: 0.90, attack_surface: 1.00
  Description: An adversary abuses the flexibility and discrepancies in the parsing and interpretation of HTTP Request messages by different intermediary HTTP agents (e.g., load balancer, reverse proxy, web caching ...

- Serialized Data with Nested Payloads
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.8
  Risk Scores: Financial: 2.6399999999999997, Safety: 2.6399999999999997, Privacy: 12.671999999999999
  Risk Factors: exposure: 0.70, complexity: 0.90, attack_surface: 1.00
  Description: Applications often need to transform data in and out of a data format (e.g., XML and YAML) by using a parser. It may be possible for an adversary to inject data that may have an adverse effect on the ...

- Command Injection
  Impact Scores: Financial: 4.8, Safety: 1, Privacy: 1
  Risk Scores: Financial: 12.671999999999999, Safety: 2.6399999999999997, Privacy: 2.6399999999999997
  Risk Factors: exposure: 0.70, complexity: 0.90, attack_surface: 1.00
  Description: An adversary looking to execute a command of their choosing, injects new items into an existing command thus modifying interpretation away from what was intended. Commands in this context are often st...

- Leveraging Race Conditions via Symbolic Links
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.8
  Risk Scores: Financial: 2.6399999999999997, Safety: 2.6399999999999997, Privacy: 12.671999999999999
  Risk Factors: exposure: 0.70, complexity: 0.90, attack_surface: 1.00
  Description: This attack leverages the use of symbolic links (Symlinks) in order to write to sensitive files. An attacker can create a Symlink link to a target file not otherwise accessible to them. When the privi...

- HTTP Response Smuggling
  Impact Scores: Financial: 4.8, Safety: 1, Privacy: 1
  Risk Scores: Financial: 12.671999999999999, Safety: 2.6399999999999997, Privacy: 2.6399999999999997
  Risk Factors: exposure: 0.70, complexity: 0.90, attack_surface: 1.00
  Description: An adversary manipulates and injects malicious content in the form of secret unauthorized HTTP responses, into a single HTTP response from a vulnerable or compromised back-end HTTP agent (e.g., server...

- SOAP Manipulation
  Impact Scores: Financial: 4.8, Safety: 1, Privacy: 1
  Risk Scores: Financial: 12.671999999999999, Safety: 2.6399999999999997, Privacy: 2.6399999999999997
  Risk Factors: exposure: 0.70, complexity: 0.90, attack_surface: 1.00
  Description: Simple Object Access Protocol (SOAP) is used as a communication protocol between a client and server

to invoke web services on the server. It is an XML-based protocol, and therefore suffers from many ...

- HTTP Request Smuggling
  Impact Scores: Financial: 4.8, Safety: 1, Privacy: 1
  Risk Scores: Financial: 12.671999999999999, Safety: 2.6399999999999997, Privacy: 2.6399999999999997
  Risk Factors: exposure: 0.70, complexity: 0.90, attack_surface: 1.00
  Description: An adversary abuses the flexibility and discrepancies in the parsing and interpretation of HTTP Request messages using various HTTP headers, request-line and body parameters as well as message sizes (...

- HTTP Response Splitting
  Impact Scores: Financial: 4.8, Safety: 1, Privacy: 1
  Risk Scores: Financial: 12.671999999999999, Safety: 2.6399999999999997, Privacy: 2.6399999999999997
  Risk Factors: exposure: 0.70, complexity: 0.90, attack_surface: 1.00
  Description: An adversary manipulates and injects malicious content, in the form of secret unauthorized HTTP responses, into a single HTTP response from a vulnerable or compromised back-end HTTP agent (e.g., web s...

- Using Alternative IP Address Encodings
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.8
  Risk Scores: Financial: 2.6399999999999997, Safety: 2.6399999999999997, Privacy: 12.671999999999999
  Risk Factors: exposure: 0.70, complexity: 0.90, attack_surface: 1.00
  Description: This attack relies on the adversary using unexpected formats for representing IP addresses. Networked applications may expect network location information in a specific format, such as fully qualified...

- Exploiting Multiple Input Interpretation Layers
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.8
  Risk Scores: Financial: 2.6399999999999997, Safety: 2.6399999999999997, Privacy: 12.671999999999999
  Risk Factors: exposure: 0.70, complexity: 0.90, attack_surface: 1.00
  Description: An attacker supplies the target software with input data that contains sequences of special characters designed to bypass input validation logic. This exploit relies on the target making multiples pas...

- Development Alteration
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.8
  Risk Scores: Financial: 2.6399999999999997, Safety: 2.6399999999999997, Privacy: 12.671999999999999
  Risk Factors: exposure: 0.70, complexity: 0.90, attack_surface: 1.00
  Description: An adversary modifies a technology, product, or component during its development to acheive a negative impact once the system is deployed. The goal of the adversary is to modify the system in such a w...

- Malicious Logic Insertion into Product Software via Configuration Management Manipulation
  Impact Scores: Financial: 4.8, Safety: 1, Privacy: 1
  Risk Scores: Financial: 12.671999999999999, Safety: 2.6399999999999997, Privacy: 2.6399999999999997
  Risk Factors: exposure: 0.70, complexity: 0.90, attack_surface: 1.00
  Description: An adversary exploits a configuration management system so that malicious logic is inserted into a software products build, update or deployed environment. If an adversary can control the elements inc...

- Design Alteration
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.8
  Risk Scores: Financial: 2.6399999999999997, Safety: 2.6399999999999997, Privacy: 12.671999999999999
  Risk Factors: exposure: 0.70, complexity: 0.90, attack_surface: 1.00
  Description: An adversary modifies the design of a technology, product, or component to acheive a negative impact once the system is deployed. In this type of attack, the goal of the adversary is to modify the des...

- Contradictory Destinations in Traffic Routing Schemes
  Impact Scores: Financial: 4.8, Safety: 1, Privacy: 1

Risk Scores: Financial: 12.671999999999999, Safety: 2.6399999999999997, Privacy: 2.6399999999999997
Risk Factors: exposure: 0.70, complexity: 0.90, attack_surface: 1.00
Description: Adversaries can provide contradictory destinations when sending messages. Traffic is routed in networks using the domain names in various headers available at different levels of the OSI model. In a C...

- Object Injection
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.8
  Risk Scores: Financial: 2.6399999999999997, Safety: 2.6399999999999997, Privacy: 12.671999999999999
  Risk Factors: exposure: 0.70, complexity: 0.90, attack_surface: 1.00
  Description: An adversary attempts to exploit an application by injecting additional, malicious content during its processing of serialized objects. Developers leverage serialization in order to convert data or st...

- Bluetooth Impersonation AttackS (BIAS)
  Impact Scores: Financial: 4.8, Safety: 1, Privacy: 1
  Risk Scores: Financial: 12.671999999999999, Safety: 2.6399999999999997, Privacy: 2.6399999999999997
  Risk Factors: exposure: 0.70, complexity: 0.90, attack_surface: 1.00
  Description: An adversary disguises the MAC address of their Bluetooth enabled device to one for which there exists an active and trusted connection and authenticates successfully. The adversary can then perform m...

- Alteration of a Software Update
  Impact Scores: Financial: 4.8, Safety: 1, Privacy: 1
  Risk Scores: Financial: 12.671999999999999, Safety: 2.6399999999999997, Privacy: 2.6399999999999997
  Risk Factors: exposure: 0.70, complexity: 0.90, attack_surface: 1.00
  Description: An adversary with access to an organization’s software update infrastructure inserts malware into the content of an outgoing update to fielded systems where a wide range of malicious effects are possi...

- Eavesdropping on a Monitor
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.8
  Risk Scores: Financial: 2.6399999999999997, Safety: 2.6399999999999997, Privacy: 12.671999999999999
  Risk Factors: exposure: 0.70, complexity: 0.90, attack_surface: 1.00
  Description: An Adversary can eavesdrop on the content of an external monitor through the air without modifying any cable or installing software, just capturing this signal emitted by the cable or video port, with...

- Browser in the Middle (BiTM)
  Impact Scores: Financial: 4.8, Safety: 1, Privacy: 1
  Risk Scores: Financial: 12.671999999999999, Safety: 2.6399999999999997, Privacy: 2.6399999999999997
  Risk Factors: exposure: 0.70, complexity: 0.90, attack_surface: 1.00
  Description: An adversary exploits the inherent functionalities of a web browser, in order to establish an unnoticed remote desktop connection in the victim's browser to the adversary's system. The adversary must ...

- Manipulating State
  Impact Scores: Financial: 1.2, Safety: 1, Privacy: 4.8
  Risk Scores: Financial: 3.1679999999999997, Safety: 2.6399999999999997, Privacy: 12.671999999999999
  Risk Factors: exposure: 0.70, complexity: 0.90, attack_surface: 1.00
  Description: The adversary modifies state information maintained by the target software or causes a state transition in hardware. If successful, the target will use this tainted state and execute in an unintended ...

- Flooding
  Impact Scores: Financial: 1, Safety: 1.2, Privacy: 3.5999999999999996
  Risk Scores: Financial: 3.5199999999999996, Safety: 4.223999999999999, Privacy: 12.671999999999997
  Risk Factors: exposure: 0.70, complexity: 0.90, attack_surface: 1.00
  Description: An adversary consumes the resources of a target by rapidly engaging in a large number of interactions with the target. This type of attack generally exposes a weakness in rate limiting or flow. When s...

- Directory Indexing
  Impact Scores: Financial: 1, Safety: 1, Privacy: 3.5999999999999996
  Risk Scores: Financial: 3.5199999999999996, Safety: 3.5199999999999996, Privacy: 12.671999999999997
  Risk Factors: exposure: 0.70, complexity: 0.90, attack_surface: 1.00
  Description: An adversary crafts a request to a target that results in the target listing/indexing the content of a directory as output. One common method of triggering directory contents as output is to construct...

- Flash Parameter Injection
  Impact Scores: Financial: 1, Safety: 1, Privacy: 3.5999999999999996
  Risk Scores: Financial: 3.5199999999999996, Safety: 3.5199999999999996, Privacy: 12.671999999999997
  Risk Factors: exposure: 0.70, complexity: 0.90, attack_surface: 1.00
  Description: An adversary takes advantage of improper data validation to inject malicious global parameters into a Flash file embedded within an HTML document. Flash files can leverage user-submitted data to confi...

- Exploiting Incorrectly Configured Access Control Security Levels
  Impact Scores: Financial: 1, Safety: 1, Privacy: 3.5999999999999996
  Risk Scores: Financial: 3.5199999999999996, Safety: 3.5199999999999996, Privacy: 12.671999999999997
  Risk Factors: exposure: 0.70, complexity: 0.90, attack_surface: 1.00
  Description: An attacker exploits a weakness in the configuration of access controls and is able to bypass the intended protection that these measures guard against and thereby obtain unauthorized access to the sy...

- Exponential Data Expansion
  Impact Scores: Financial: 1, Safety: 1, Privacy: 3.5999999999999996
  Risk Scores: Financial: 3.5199999999999996, Safety: 3.5199999999999996, Privacy: 12.671999999999997
  Risk Factors: exposure: 0.70, complexity: 0.90, attack_surface: 1.00
  Description: An adversary submits data to a target application which contains nested exponential data expansion to produce excessively large output. Many data format languages allow the definition of macro-like st...

- Inducing Account Lockout
  Impact Scores: Financial: 1, Safety: 1, Privacy: 3.5999999999999996
  Risk Scores: Financial: 3.5199999999999996, Safety: 3.5199999999999996, Privacy: 12.671999999999997
  Risk Factors: exposure: 0.70, complexity: 0.90, attack_surface: 1.00
  Description: An attacker leverages the security functionality of the system aimed at thwarting potential attacks to launch a denial of service attack against a legitimate system user. Many systems, for instance, i...

- XML Routing Detour Attacks
  Impact Scores: Financial: 1, Safety: 1, Privacy: 3.5999999999999996
  Risk Scores: Financial: 3.5199999999999996, Safety: 3.5199999999999996, Privacy: 12.671999999999997
  Risk Factors: exposure: 0.70, complexity: 0.90, attack_surface: 1.00
  Description: An attacker subverts an intermediate system used to process XML content and forces the intermediate to modify and/or re-route the processing of the content. XML Routing Detour Attacks are Adversary in...

- Fuzzing
  Impact Scores: Financial: 1, Safety: 1, Privacy: 3.5999999999999996
  Risk Scores: Financial: 3.5199999999999996, Safety: 3.5199999999999996, Privacy: 12.671999999999997
  Risk Factors: exposure: 0.70, complexity: 0.90, attack_surface: 1.00
  Description: In this attack pattern, the adversary leverages fuzzing to try to identify weaknesses in the system. Fuzzing is a software security and functionality testing method that feeds randomly constructed inp...

- Manipulating Opaque Client-based Data Tokens
  Impact Scores: Financial: 1, Safety: 1, Privacy: 3.5999999999999996
  Risk Scores: Financial: 3.5199999999999996, Safety: 3.5199999999999996, Privacy: 12.671999999999997
  Risk Factors: exposure: 0.70, complexity: 0.90, attack_surface: 1.00

Description: In circumstances where an application holds important data client-side in tokens (cookies, URLs, data files, and so forth) that data can be manipulated. If client or server-side application components...

- Interface Manipulation
  Impact Scores: Financial: 3.5999999999999996, Safety: 1, Privacy: 1
  Risk Scores: Financial: 9.503999999999998, Safety: 2.6399999999999997, Privacy: 2.6399999999999997
  Risk Factors: exposure: 0.70, complexity: 0.90, attack_surface: 1.00
  Description: An adversary manipulates the use or processing of an interface (e.g. Application Programming Interface (API) or System-on-Chip (SoC)) resulting in an adverse impact upon the security of the system imp...

- Parameter Injection
  Impact Scores: Financial: 1, Safety: 1, Privacy: 3.5999999999999996
  Risk Scores: Financial: 2.6399999999999997, Safety: 2.6399999999999997, Privacy: 9.503999999999998
  Risk Factors: exposure: 0.70, complexity: 0.90, attack_surface: 1.00
  Description: An adversary manipulates the content of request parameters for the purpose of undermining the security of the target. Some parameter encodings use text characters as separators. For example, parameter...

- Content Spoofing
  Impact Scores: Financial: 3.5999999999999996, Safety: 1, Privacy: 3.5999999999999996
  Risk Scores: Financial: 9.503999999999998, Safety: 2.6399999999999997, Privacy: 9.503999999999998
  Risk Factors: exposure: 0.70, complexity: 0.90, attack_surface: 1.00
  Description: An adversary modifies content to make it contain something other than what the original content producer intended while keeping the apparent source of the content unchanged. The term content spoofing ...

- Resource Location Spoofing
  Impact Scores: Financial: 1, Safety: 1, Privacy: 3.5999999999999996
  Risk Scores: Financial: 2.6399999999999997, Safety: 2.6399999999999997, Privacy: 9.503999999999998
  Risk Factors: exposure: 0.70, complexity: 0.90, attack_surface: 1.00
  Description: An adversary deceives an application or user and convinces them to request a resource from an unintended location. By spoofing the location, the adversary can cause an alternate resource to be used, o...

- Cross-Site Flashing
  Impact Scores: Financial: 3.5999999999999996, Safety: 1, Privacy: 1
  Risk Scores: Financial: 9.503999999999998, Safety: 2.6399999999999997, Privacy: 2.6399999999999997
  Risk Factors: exposure: 0.70, complexity: 0.90, attack_surface: 1.00
  Description: An attacker is able to trick the victim into executing a Flash document that passes commands or calls to a Flash player browser plugin, allowing the attacker to exploit native Flash functionality in t...

- Modification of Registry Run Keys
  Impact Scores: Financial: 1, Safety: 1, Privacy: 3.5999999999999996
  Risk Scores: Financial: 2.6399999999999997, Safety: 2.6399999999999997, Privacy: 9.503999999999998
  Risk Factors: exposure: 0.70, complexity: 0.90, attack_surface: 1.00
  Description: An adversary adds a new entry to the run keys in the Windows registry so that an application of their choosing is executed when a user logs in. In this way, the adversary can get their executable to o...

- Using Leading 'Ghost' Character Sequences to Bypass Input Filters
  Impact Scores: Financial: 1, Safety: 1, Privacy: 3.5999999999999996
  Risk Scores: Financial: 2.6399999999999997, Safety: 2.6399999999999997, Privacy: 9.503999999999998
  Risk Factors: exposure: 0.70, complexity: 0.90, attack_surface: 1.00
  Description: Some APIs will strip certain leading characters from a string of parameters. An adversary can intentionally introduce leading ghost characters (extra characters that don't affect the validity of the r...

- Manipulate Human Behavior

Impact Scores: Financial: 1, Safety: 1, Privacy: 3.5999999999999996
Risk Scores: Financial: 2.6399999999999997, Safety: 2.6399999999999997, Privacy: 9.503999999999998
Risk Factors: exposure: 0.70, complexity: 0.90, attack_surface: 1.00
Description: An adversary exploits inherent human psychological predisposition to influence a targeted individual or group to solicit information or manipulate the target into performing an action that serves the ...

- Disable Security Software
Impact Scores: Financial: 3.5999999999999996, Safety: 1, Privacy: 1
Risk Scores: Financial: 9.503999999999998, Safety: 2.6399999999999997, Privacy: 2.6399999999999997
Risk Factors: exposure: 0.70, complexity: 0.90, attack_surface: 1.00
Description: An adversary exploits a weakness in access control to disable security tools so that detection does not occur. This can take the form of killing processes, deleting registry keys so that tools do not ...

- Collect Data from Registries
Impact Scores: Financial: 1, Safety: 1, Privacy: 3.5999999999999996
Risk Scores: Financial: 2.6399999999999997, Safety: 2.6399999999999997, Privacy: 9.503999999999998
Risk Factors: exposure: 0.70, complexity: 0.90, attack_surface: 1.00
Description: An adversary exploits a weakness in authorization to gather system-specific data and sensitive information within a registry (e.g., Windows Registry, Mac plist). These contain information about the sy...

- Collect Data from Screen Capture
Impact Scores: Financial: 1, Safety: 1, Privacy: 3.5999999999999996
Risk Scores: Financial: 2.6399999999999997, Safety: 2.6399999999999997, Privacy: 9.503999999999998
Risk Factors: exposure: 0.70, complexity: 0.90, attack_surface: 1.00
Description: An adversary gathers sensitive information by exploiting the system's screen capture functionality. Through screenshots, the adversary aims to see what happens on the screen over the course of an oper...

- Retrieve Data from Decommissioned Devices
Impact Scores: Financial: 1, Safety: 1.2, Privacy: 3.5999999999999996
Risk Scores: Financial: 2.6399999999999997, Safety: 3.1679999999999997, Privacy: 9.503999999999998
Risk Factors: exposure: 0.70, complexity: 0.90, attack_surface: 1.00
Description: An adversary obtains decommissioned, recycled, or discarded systems and devices that can include an organization’s intellectual property, employee data, and other types of controlled information. Syst...

- Escaping a Sandbox by Calling Code in Another Language
Impact Scores: Financial: 1, Safety: 1, Privacy: 5
Risk Scores: Financial: 1.7599999999999998, Safety: 1.7599999999999998, Privacy: 8.799999999999999
Risk Factors: exposure: 0.70, complexity: 0.90, attack_surface: 1.00
Description: The attacker may submit malicious code of another language to obtain access to privileges that were not intentionally exposed by the sandbox, thus escaping the sandbox. For instance, Java code cannot ...

- Hijacking a Privileged Thread of Execution
Impact Scores: Financial: 5, Safety: 1, Privacy: 1
Risk Scores: Financial: 8.799999999999999, Safety: 1.7599999999999998, Privacy: 1.7599999999999998
Risk Factors: exposure: 0.70, complexity: 0.90, attack_surface: 1.00
Description: An adversary hijacks a privileged thread of execution by injecting malicious code into a running process. By using a privleged thread to do their bidding, adversaries can evade process-based detection...

- Subvert Code-signing Facilities
Impact Scores: Financial: 1, Safety: 1, Privacy: 5
Risk Scores: Financial: 1.7599999999999998, Safety: 1.7599999999999998, Privacy: 8.799999999999999
Risk Factors: exposure: 0.70, complexity: 0.90, attack_surface: 1.00
Description: Many languages use code signing facilities to vouch for code's identity and to thus tie code to its assigned

privileges within an environment. Subverting this mechanism can be instrumental in an attac...

- Load Value Injection
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5
  Risk Scores: Financial: 1.7599999999999998, Safety: 1.7599999999999998, Privacy: 8.799999999999999
  Risk Factors: exposure: 0.70, complexity: 0.90, attack_surface: 1.00
  Description: An adversary exploits a hardware design flaw in a CPU implementation of transient instruction execution in which a faulting or assisted load instruction transiently forwards adversary-controlled data ...

- Web Application Fingerprinting
  Impact Scores: Financial: 1, Safety: 1, Privacy: 2.4
  Risk Scores: Financial: 3.5199999999999996, Safety: 3.5199999999999996, Privacy: 8.447999999999999
  Risk Factors: exposure: 0.70, complexity: 0.90, attack_surface: 1.00
  Description: An attacker sends a series of probes to a web application in order to elicit version-dependent and type-dependent behavior that assists in identifying the target. An attacker could learn information s...

- Fuzzing for application mapping
  Impact Scores: Financial: 1, Safety: 2.4, Privacy: 1
  Risk Scores: Financial: 3.5199999999999996, Safety: 8.447999999999999, Privacy: 3.5199999999999996
  Risk Factors: exposure: 0.70, complexity: 0.90, attack_surface: 1.00
  Description: An attacker sends random, malformed, or otherwise unexpected messages to a target application and observes the application's log or error messages returned. The attacker does not initially know how a ...

- Forced Deadlock
  Impact Scores: Financial: 4.8, Safety: 1, Privacy: 1
  Risk Scores: Financial: 8.447999999999999, Safety: 1.7599999999999998, Privacy: 1.7599999999999998
  Risk Factors: exposure: 0.70, complexity: 0.90, attack_surface: 1.00
  Description: The adversary triggers and exploits a deadlock condition in the target software to cause a denial of service. A deadlock can occur when two or more competing actions are waiting for each other to fini...

- Schema Poisoning
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.8
  Risk Scores: Financial: 1.7599999999999998, Safety: 1.7599999999999998, Privacy: 8.447999999999999
  Risk Factors: exposure: 0.70, complexity: 0.90, attack_surface: 1.00
  Description: An adversary corrupts or modifies the content of a schema for the purpose of undermining the security of the target. Schemas provide the structure and content definitions for resources used by an appl...

- USB Memory Attacks
  Impact Scores: Financial: 2.4, Safety: 1, Privacy: 4.8
  Risk Scores: Financial: 4.223999999999999, Safety: 1.7599999999999998, Privacy: 8.447999999999999
  Risk Factors: exposure: 0.70, complexity: 0.90, attack_surface: 1.00
  Description: An adversary loads malicious code onto a USB memory stick in order to infect any system which the device is plugged in to. USB drives present a significant security risk for business and government ag...

- Signature Spoofing by Misrepresentation
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.8
  Risk Scores: Financial: 1.7599999999999998, Safety: 1.7599999999999998, Privacy: 8.447999999999999
  Risk Factors: exposure: 0.70, complexity: 0.90, attack_surface: 1.00
  Description: An attacker exploits a weakness in the parsing or display code of the recipient software to generate a data blob containing a supposedly valid signature, but the signer's identity is falsely represent...

- Hardware Component Substitution During Baselining
  Impact Scores: Financial: 4.8, Safety: 1, Privacy: 1

Risk Scores: Financial: 8.447999999999999, Safety: 1.7599999999999998, Privacy: 1.7599999999999998
Risk Factors: exposure: 0.70, complexity: 0.90, attack_surface: 1.00
Description: An adversary with access to system components during allocated baseline development can substitute a maliciously altered hardware component for a baseline component during the product development and ...

- Malicious Hardware Update
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.8
  Risk Scores: Financial: 1.7599999999999998, Safety: 1.7599999999999998, Privacy: 8.447999999999999
  Risk Factors: exposure: 0.70, complexity: 0.90, attack_surface: 1.00
  Description: An adversary introduces malicious hardware during an update or replacement procedure, allowing for additional compromise or site disruption at the victim location. After deployment, it is not uncommon...

- Open-Source Library Manipulation
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.8
  Risk Scores: Financial: 1.7599999999999998, Safety: 1.7599999999999998, Privacy: 8.447999999999999
  Risk Factors: exposure: 0.70, complexity: 0.90, attack_surface: 1.00
  Description: Adversaries implant malicious code in open source software (OSS) libraries to have it widely distributed, as OSS is commonly downloaded by developers and other users to incorporate into software devel...

- ASIC With Malicious Functionality
  Impact Scores: Financial: 4.8, Safety: 1, Privacy: 1
  Risk Scores: Financial: 8.447999999999999, Safety: 1.7599999999999998, Privacy: 1.7599999999999998
  Risk Factors: exposure: 0.70, complexity: 0.90, attack_surface: 1.00
  Description: An attacker with access to the development environment process of an application-specific integrated circuit (ASIC) for a victim system being developed or maintained after initial deployment can inser...

- Hardware Fault Injection
  Impact Scores: Financial: 1, Safety: 4.8, Privacy: 4.8
  Risk Scores: Financial: 1.7599999999999998, Safety: 8.447999999999999, Privacy: 8.447999999999999
  Risk Factors: exposure: 0.70, complexity: 0.90, attack_surface: 1.00
  Description: The adversary uses disruptive signals or events, or alters the physical environment a device operates in, to cause faulty behavior in electronic devices. This can include electromagnetic pulses, laser...

- Carry-Off GPS Attack
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.8
  Risk Scores: Financial: 1.7599999999999998, Safety: 1.7599999999999998, Privacy: 8.447999999999999
  Risk Factors: exposure: 0.70, complexity: 0.90, attack_surface: 1.00
  Description: A common form of a GPS spoofing attack, commonly termed a carry-off attack begins with an adversary broadcasting signals synchronized with the genuine signals observed by the target receiver. The powe...

- DLL Side-Loading
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.8
  Risk Scores: Financial: 1.7599999999999998, Safety: 1.7599999999999998, Privacy: 8.447999999999999
  Risk Factors: exposure: 0.70, complexity: 0.90, attack_surface: 1.00
  Description: An adversary places a malicious version of a Dynamic-Link Library (DLL) in the Windows Side-by-Side (WinSxS) directory to trick the operating system into loading this malicious DLL instead of a legiti...

- Use of Captured Tickets (Pass The Ticket)
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.8
  Risk Scores: Financial: 1.7599999999999998, Safety: 1.7599999999999998, Privacy: 8.447999999999999
  Risk Factors: exposure: 0.70, complexity: 0.90, attack_surface: 1.00
  Description: An adversary uses stolen Kerberos tickets to access systems/resources that leverage the Kerberos authentication protocol. The Kerberos authentication protocol centers around a ticketing system which i...

- Sniff Application Code
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.8
  Risk Scores: Financial: 1.7599999999999998, Safety: 1.7599999999999998, Privacy: 8.447999999999999
  Risk Factors: exposure: 0.70, complexity: 0.90, attack_surface: 1.00
  Description: An adversary passively sniffs network communications and captures application code bound for an authorized client. Once obtained, they can use it as-is, or through reverse-engineering glean sensitive ...

- Key Negotiation of Bluetooth Attack (KNOB)
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.8
  Risk Scores: Financial: 1.7599999999999998, Safety: 1.7599999999999998, Privacy: 8.447999999999999
  Risk Factors: exposure: 0.70, complexity: 0.90, attack_surface: 1.00
  Description: An adversary can exploit a flaw in Bluetooth key negotiation allowing them to decrypt information sent between two devices communicating via Bluetooth. The adversary uses an Adversary in the Middle se...

- Malicious Code Implanted During Chip Programming
  Impact Scores: Financial: 4.8, Safety: 1, Privacy: 1
  Risk Scores: Financial: 8.447999999999999, Safety: 1.7599999999999998, Privacy: 1.7599999999999998
  Risk Factors: exposure: 0.70, complexity: 0.90, attack_surface: 1.00
  Description: During the programming step of chip manufacture, an adversary with access and necessary technical skills maliciously alters a chip's intended program logic to produce an effect intended by the adversa...

- AJAX Footprinting
  Impact Scores: Financial: 1, Safety: 1, Privacy: 2.4
  Risk Scores: Financial: 3.5199999999999996, Safety: 3.5199999999999996, Privacy: 8.447999999999999
  Risk Factors: exposure: 0.70, complexity: 0.90, attack_surface: 1.00
  Description: This attack utilizes the frequent client-server roundtrips in Ajax conversation to scan a system. While Ajax does not open up new vulnerabilities per se, it does optimize them from an attacker point o...

- Active OS Fingerprinting
  Impact Scores: Financial: 1, Safety: 1, Privacy: 2.4
  Risk Scores: Financial: 2.6399999999999997, Safety: 2.6399999999999997, Privacy: 6.335999999999999
  Risk Factors: exposure: 0.70, complexity: 0.90, attack_surface: 1.00
  Description: An adversary engages in activity to detect the operating system or firmware version of a remote target by interrogating a device, server, or platform with a probe designed to solicit behavior that wil...

- TCP Timestamp Probe
  Impact Scores: Financial: 2.4, Safety: 1, Privacy: 1
  Risk Scores: Financial: 6.335999999999999, Safety: 2.6399999999999997, Privacy: 2.6399999999999997
  Risk Factors: exposure: 0.70, complexity: 0.90, attack_surface: 1.00
  Description: This OS fingerprinting probe examines the remote server's implementation of TCP timestamps. Not all operating systems implement timestamps within the TCP header, but when timestamps are used then this...

- TCP Sequence Number Probe
  Impact Scores: Financial: 2.4, Safety: 1, Privacy: 1
  Risk Scores: Financial: 6.335999999999999, Safety: 2.6399999999999997, Privacy: 2.6399999999999997
  Risk Factors: exposure: 0.70, complexity: 0.90, attack_surface: 1.00
  Description: This OS fingerprinting probe tests the target system's assignment of TCP sequence numbers. One common way to test TCP Sequence Number generation is to send a probe packet to an open port on the target...

- TCP (ISN) Greatest Common Divisor Probe
  Impact Scores: Financial: 1, Safety: 1, Privacy: 2.4
  Risk Scores: Financial: 2.6399999999999997, Safety: 2.6399999999999997, Privacy: 6.335999999999999
  Risk Factors: exposure: 0.70, complexity: 0.90, attack_surface: 1.00

Description: This OS fingerprinting probe sends a number of TCP SYN packets to an open port of a remote machine. The Initial Sequence Number (ISN) in each of the SYN/ACK response packets is analyzed to determine t...

- TCP (ISN) Counter Rate Probe
  Impact Scores: Financial: 1, Safety: 1, Privacy: 2.4
  Risk Scores: Financial: 2.6399999999999997, Safety: 2.6399999999999997, Privacy: 6.335999999999999
  Risk Factors: exposure: 0.70, complexity: 0.90, attack_surface: 1.00
  Description: This OS detection probe measures the average rate of initial sequence number increments during a period of time. Sequence numbers are incremented using a time-based algorithm and are susceptible to a ...

- TCP (ISN) Sequence Predictability Probe
  Impact Scores: Financial: 1, Safety: 1, Privacy: 2.4
  Risk Scores: Financial: 2.6399999999999997, Safety: 2.6399999999999997, Privacy: 6.335999999999999
  Risk Factors: exposure: 0.70, complexity: 0.90, attack_surface: 1.00
  Description: This type of operating system probe attempts to determine an estimate for how predictable the sequence number generation algorithm is for a remote host. Statistical techniques, such as standard deviat...

- TCP Initial Window Size Probe
  Impact Scores: Financial: 2.4, Safety: 1, Privacy: 1
  Risk Scores: Financial: 6.335999999999999, Safety: 2.6399999999999997, Privacy: 2.6399999999999997
  Risk Factors: exposure: 0.70, complexity: 0.90, attack_surface: 1.00
  Description: This OS fingerprinting probe checks the initial TCP Window size. TCP stacks limit the range of sequence numbers allowable within a session to maintain the connected state within TCP protocol logic. Th...

- TCP Options Probe
  Impact Scores: Financial: 2.4, Safety: 1, Privacy: 1
  Risk Scores: Financial: 6.335999999999999, Safety: 2.6399999999999997, Privacy: 2.6399999999999997
  Risk Factors: exposure: 0.70, complexity: 0.90, attack_surface: 1.00
  Description: This OS fingerprinting probe analyzes the type and order of any TCP header options present within a response segment. Most operating systems use unique ordering and different option sets when options ...

- Pretexting
  Impact Scores: Financial: 1, Safety: 1, Privacy: 2.4
  Risk Scores: Financial: 2.6399999999999997, Safety: 2.6399999999999997, Privacy: 6.335999999999999
  Risk Factors: exposure: 0.70, complexity: 0.90, attack_surface: 1.00
  Description: An adversary engages in pretexting behavior to solicit information from target persons, or manipulate the target into performing some action that serves the adversary's interests. During a pretexting ...

- Interception
  Impact Scores: Financial: 1, Safety: 1, Privacy: 3.5999999999999996
  Risk Scores: Financial: 1.7599999999999998, Safety: 1.7599999999999998, Privacy: 6.3359999999999985
  Risk Factors: exposure: 0.70, complexity: 0.90, attack_surface: 1.00
  Description: An adversary monitors data streams to or from the target for information gathering purposes. This attack may be undertaken to solely gather sensitive information or to support a further attack against...

- XML Ping of the Death
  Impact Scores: Financial: 1, Safety: 3.5999999999999996, Privacy: 1
  Risk Scores: Financial: 1.7599999999999998, Safety: 6.3359999999999985, Privacy: 1.7599999999999998
  Risk Factors: exposure: 0.70, complexity: 0.90, attack_surface: 1.00
  Description: An attacker initiates a resource depletion attack where a large number of small XML messages are delivered at a sufficiently rapid rate to cause a denial of service or crash of the target. Transaction...

- Incomplete Data Deletion in a Multi-Tenant Environment

Impact Scores: Financial: 1, Safety: 1, Privacy: 3.5999999999999996
Risk Scores: Financial: 1.7599999999999998, Safety: 1.7599999999999998, Privacy: 6.3359999999999985
Risk Factors: exposure: 0.70, complexity: 0.90, attack_surface: 1.00
Description: An adversary obtains unauthorized information due to insecure or incomplete data deletion in a multi-tenant environment. If a cloud provider fails to completely delete storage and data from former clo...

- Adding a Space to a File Extension
Impact Scores: Financial: 1, Safety: 1, Privacy: 3.5999999999999996
Risk Scores: Financial: 1.7599999999999998, Safety: 1.7599999999999998, Privacy: 6.3359999999999985
Risk Factors: exposure: 0.70, complexity: 0.90, attack_surface: 1.00
Description: An adversary adds a space character to the end of a file extension and takes advantage of an application that does not properly neutralize trailing special elements in file names. This extra space, wh...

- Reverse Engineering
Impact Scores: Financial: 2.4, Safety: 1, Privacy: 1
Risk Scores: Financial: 4.223999999999999, Safety: 1.7599999999999998, Privacy: 1.7599999999999998
Risk Factors: exposure: 0.70, complexity: 0.90, attack_surface: 1.00
Description: An adversary discovers the structure, function, and composition of an object, resource, or system by using a variety of analysis techniques to effectively determine how the analyzed entity was constru...

- Fingerprinting
Impact Scores: Financial: 1, Safety: 1, Privacy: 1.2
Risk Scores: Financial: 3.5199999999999996, Safety: 3.5199999999999996, Privacy: 4.223999999999999
Risk Factors: exposure: 0.70, complexity: 0.90, attack_surface: 1.00
Description: An adversary compares output from a target system to known indicators that uniquely identify specific details about the target. Most commonly, fingerprinting is done to determine operating system and ...

- Target Influence via Framing
Impact Scores: Financial: 1, Safety: 1.2, Privacy: 2.4
Risk Scores: Financial: 1.7599999999999998, Safety: 2.1119999999999997, Privacy: 4.223999999999999
Risk Factors: exposure: 0.70, complexity: 0.90, attack_surface: 1.00
Description: An adversary uses framing techniques to contextualize a conversation so that the target is more likely to be influenced by the adversary's point of view. Framing is information and experiences in life...

- Influence via Psychological Principles
Impact Scores: Financial: 2.4, Safety: 1, Privacy: 1
Risk Scores: Financial: 4.223999999999999, Safety: 1.7599999999999998, Privacy: 1.7599999999999998
Risk Factors: exposure: 0.70, complexity: 0.90, attack_surface: 1.00
Description: The adversary shapes the target's actions or behavior by focusing on the ways human interact and learn, leveraging such elements as cognitive and social psychology. In a variety of ways, a target can ...

- Process Footprinting
Impact Scores: Financial: 1, Safety: 1, Privacy: 2.4
Risk Scores: Financial: 1.7599999999999998, Safety: 1.7599999999999998, Privacy: 4.223999999999999
Risk Factors: exposure: 0.70, complexity: 0.90, attack_surface: 1.00
Description: An adversary exploits functionality meant to identify information about the currently running processes on the target system to an authorized user. By knowing what processes are running on the target ...

- Services Footprinting
Impact Scores: Financial: 1, Safety: 1, Privacy: 2.4
Risk Scores: Financial: 1.7599999999999998, Safety: 1.7599999999999998, Privacy: 4.223999999999999
Risk Factors: exposure: 0.70, complexity: 0.90, attack_surface: 1.00
Description: An adversary exploits functionality meant to identify information about the services on the target system to

an authorized user. By knowing what services are registered on the target system, the adver...

- Account Footprinting
  Impact Scores: Financial: 1, Safety: 1, Privacy: 2.4
  Risk Scores: Financial: 1.7599999999999998, Safety: 1.7599999999999998, Privacy: 4.223999999999999
  Risk Factors: exposure: 0.70, complexity: 0.90, attack_surface: 1.00
  Description: An adversary exploits functionality meant to identify information about the domain accounts and their permissions on the target system to an authorized user. By knowing what accounts are registered on...

- Group Permission Footprinting
  Impact Scores: Financial: 1, Safety: 1, Privacy: 2.4
  Risk Scores: Financial: 1.7599999999999998, Safety: 1.7599999999999998, Privacy: 4.223999999999999
  Risk Factors: exposure: 0.70, complexity: 0.90, attack_surface: 1.00
  Description: An adversary exploits functionality meant to identify information about user groups and their permissions on the target system to an authorized user. By knowing what users/permissions are registered o...

- Owner Footprinting
  Impact Scores: Financial: 1, Safety: 1, Privacy: 2.4
  Risk Scores: Financial: 1.7599999999999998, Safety: 1.7599999999999998, Privacy: 4.223999999999999
  Risk Factors: exposure: 0.70, complexity: 0.90, attack_surface: 1.00
  Description: An adversary exploits functionality meant to identify information about the primary users on the target system to an authorized user. They may do this, for example, by reviewing logins or file modific...

- System Footprinting
  Impact Scores: Financial: 1, Safety: 1, Privacy: 2.4
  Risk Scores: Financial: 1.7599999999999998, Safety: 1.7599999999999998, Privacy: 4.223999999999999
  Risk Factors: exposure: 0.70, complexity: 0.90, attack_surface: 1.00
  Description: An adversary engages in active probing and exploration activities to determine security information about a remote target system. Often times adversaries will rely on remote applications that can be p...

- Collect Data from Clipboard
  Impact Scores: Financial: 1, Safety: 1, Privacy: 2.4
  Risk Scores: Financial: 1.7599999999999998, Safety: 1.7599999999999998, Privacy: 4.223999999999999
  Risk Factors: exposure: 0.70, complexity: 0.90, attack_surface: 1.00
  Description: The adversary exploits an application that allows for the copying of sensitive data or information by collecting information copied to the clipboard. Data copied to the clipboard can be accessed by ot...

Component: CAN Bus Network

Type: Network
Safety Level: ASIL C
Interfaces: CAN
Access Points:
Data Types: All Traffic
Location: Internal
Trust Zone: Standard
Connected To: GWY001, ECU003, ECU001, ECU002

Identified Threats:

- Buffer Manipulation

Impact Scores: Financial: 1, Safety: 1, Privacy: 5
Risk Scores: Financial: 2.4, Safety: 2.4, Privacy: 12.0
Risk Factors: exposure: 0.60, complexity: 0.60, attack_surface: 0.20
Description: An adversary manipulates an application's interaction with a buffer in an attempt to read or modify data they shouldn't have access to. Buffer attacks are distinguished in that it is the buffer space ...

- Redirect Access to Libraries
  Impact Scores: Financial: 1, Safety: 5, Privacy: 1
  Risk Scores: Financial: 2.4, Safety: 12.0, Privacy: 2.4
  Risk Factors: exposure: 0.60, complexity: 0.60, attack_surface: 0.20
  Description: An adversary exploits a weakness in the way an application searches for external libraries to manipulate the execution flow to point to an adversary supplied library or code base. This pattern of atta...

- XSS Targeting Non-Script Elements
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5
  Risk Scores: Financial: 2.4, Safety: 2.4, Privacy: 12.0
  Risk Factors: exposure: 0.60, complexity: 0.60, attack_surface: 0.20
  Description: This attack is a form of Cross-Site Scripting (XSS) where malicious scripts are embedded in elements that are not expected to host scripts such as image tags (<img>), comments in XML documents (< !-CD...

- Retrieve Embedded Sensitive Data
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5
  Risk Scores: Financial: 2.4, Safety: 2.4, Privacy: 12.0
  Risk Factors: exposure: 0.60, complexity: 0.60, attack_surface: 0.20
  Description: An attacker examines a target system to find sensitive data that has been embedded within it. This information can reveal confidential contents, such as account numbers or individual keys/credentials ...

- Leveraging/Manipulating Configuration File Search Paths
  Impact Scores: Financial: 5, Safety: 1, Privacy: 1
  Risk Scores: Financial: 12.0, Safety: 2.4, Privacy: 2.4
  Risk Factors: exposure: 0.60, complexity: 0.60, attack_surface: 0.20
  Description: This pattern of attack sees an adversary load a malicious resource into a program's standard path so that when a known command is executed then the system instead executes the malicious component. The...

- Manipulating Writeable Terminal Devices
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5
  Risk Scores: Financial: 2.4, Safety: 2.4, Privacy: 12.0
  Risk Factors: exposure: 0.60, complexity: 0.60, attack_surface: 0.20
  Description: This attack exploits terminal devices that allow themselves to be written to by other users. The attacker sends command strings to the target terminal device hoping that the target user will hit enter...

- Overflow Binary Resource File
  Impact Scores: Financial: 5, Safety: 1, Privacy: 1
  Risk Scores: Financial: 12.0, Safety: 2.4, Privacy: 2.4
  Risk Factors: exposure: 0.60, complexity: 0.60, attack_surface: 0.20
  Description: An attack of this type exploits a buffer overflow vulnerability in the handling of binary resources. Binary resources may include music files like MP3, image files like JPEG files, and any other binar...

- Poison Web Service Registry
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5
  Risk Scores: Financial: 2.4, Safety: 2.4, Privacy: 12.0
  Risk Factors: exposure: 0.60, complexity: 0.60, attack_surface: 0.20
  Description: SOA and Web Services often use a registry to perform look up, get schema information, and metadata

about services. A poisoned registry can redirect (think phishing for servers) the service requester t...

- String Format Overflow in syslog()
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5
  Risk Scores: Financial: 2.4, Safety: 2.4, Privacy: 12.0
  Risk Factors: exposure: 0.60, complexity: 0.60, attack_surface: 0.20
  Description: This attack targets applications and software that uses the syslog() function insecurely. If an application does not explicitely use a format string parameter in a call to syslog(), user input can be ...

- Manipulating User-Controlled Variables
  Impact Scores: Financial: 2.4, Safety: 1, Privacy: 5
  Risk Scores: Financial: 5.76, Safety: 2.4, Privacy: 12.0
  Risk Factors: exposure: 0.60, complexity: 0.60, attack_surface: 0.20
  Description: This attack targets user controlled variables (DEBUG=1, PHP Globals, and So Forth). An adversary can override variables leveraging user-supplied, untrusted query variables directly used on the applica...

- XQuery Injection
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5
  Risk Scores: Financial: 2.4, Safety: 2.4, Privacy: 12.0
  Risk Factors: exposure: 0.60, complexity: 0.60, attack_surface: 0.20
  Description: This attack utilizes XQuery to probe and attack server systems; in a similar manner that SQL Injection allows an attacker to exploit SQL calls to RDBMS, XQuery Injection uses improperly validated data...

- Pharming
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5
  Risk Scores: Financial: 2.4, Safety: 2.4, Privacy: 12.0
  Risk Factors: exposure: 0.60, complexity: 0.60, attack_surface: 0.20
  Description: A pharming attack occurs when the victim is fooled into entering sensitive data into supposedly trusted locations, such as an online bank site or a trading platform. An attacker can impersonate these ...

- Phishing
  Impact Scores: Financial: 1.2, Safety: 1, Privacy: 5
  Risk Scores: Financial: 2.88, Safety: 2.4, Privacy: 12.0
  Risk Factors: exposure: 0.60, complexity: 0.60, attack_surface: 0.20
  Description: Phishing is a social engineering technique where an attacker masquerades as a legitimate entity with which the victim might do business in order to prompt the user to reveal some confidential informat...

- Accessing Functionality Not Properly Constrained by ACLs
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.8
  Risk Scores: Financial: 2.4, Safety: 2.4, Privacy: 11.52
  Risk Factors: exposure: 0.60, complexity: 0.60, attack_surface: 0.20
  Description: In applications, particularly web applications, access to functionality is mitigated by an authorization framework. This framework maps Access Control Lists (ACLs) to elements of the application's fun...

- Buffer Overflow via Environment Variables
  Impact Scores: Financial: 4.8, Safety: 1, Privacy: 1
  Risk Scores: Financial: 11.52, Safety: 2.4, Privacy: 2.4
  Risk Factors: exposure: 0.60, complexity: 0.60, attack_surface: 0.20
  Description: This attack pattern involves causing a buffer overflow through manipulation of environment variables. Once the adversary finds that they can modify an environment variable, they may try to overflow as...

- Server Side Include (SSI) Injection
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.8

Risk Scores: Financial: 2.4, Safety: 2.4, Privacy: 11.52
Risk Factors: exposure: 0.60, complexity: 0.60, attack_surface: 0.20
Description: An attacker can use Server Side Include (SSI) Injection to send code to a web application that then gets executed by the web server. Doing so enables the attacker to achieve similar results to Cross S...

- Format String Injection
Impact Scores: Financial: 1, Safety: 2.4, Privacy: 4.8
Risk Scores: Financial: 2.4, Safety: 5.76, Privacy: 11.52
Risk Factors: exposure: 0.60, complexity: 0.60, attack_surface: 0.20
Description: An adversary includes formatting characters in a string input field on the target application. Most applications assume that users will provide static text and may respond unpredictably to the presenc...

- Cache Poisoning
Impact Scores: Financial: 1, Safety: 1, Privacy: 4.8
Risk Scores: Financial: 2.4, Safety: 2.4, Privacy: 11.52
Risk Factors: exposure: 0.60, complexity: 0.60, attack_surface: 0.20
Description: An attacker exploits the functionality of cache technologies to cause specific data to be cached that aids the attackers' objectives. This describes any attack whereby an attacker places incorrect or ...

- DNS Cache Poisoning
Impact Scores: Financial: 4.8, Safety: 1, Privacy: 1
Risk Scores: Financial: 11.52, Safety: 2.4, Privacy: 2.4
Risk Factors: exposure: 0.60, complexity: 0.60, attack_surface: 0.20
Description: A domain name server translates a domain name (such as www.example.com) into an IP address that Internet hosts use to contact Internet resources. An adversary modifies a public DNS cache to cause cert...

- Command Delimiters
Impact Scores: Financial: 1, Safety: 1, Privacy: 4.8
Risk Scores: Financial: 2.4, Safety: 2.4, Privacy: 11.52
Risk Factors: exposure: 0.60, complexity: 0.60, attack_surface: 0.20
Description: An attack of this type exploits a programs' vulnerabilities that allows an attacker's commands to be concatenated onto a legitimate command with the intent of targeting other resources such as the fil...

- Malicious Automated Software Update via Redirection
Impact Scores: Financial: 1, Safety: 1, Privacy: 4.8
Risk Scores: Financial: 2.4, Safety: 2.4, Privacy: 11.52
Risk Factors: exposure: 0.60, complexity: 0.60, attack_surface: 0.20
Description: An attacker exploits two layers of weaknesses in server or client software for automated update mechanisms to undermine the integrity of the target code-base. The first weakness involves a failure to ...

- PHP Remote File Inclusion
Impact Scores: Financial: 1, Safety: 1, Privacy: 4.8
Risk Scores: Financial: 2.4, Safety: 2.4, Privacy: 11.52
Risk Factors: exposure: 0.60, complexity: 0.60, attack_surface: 0.20
Description: In this pattern the adversary is able to load and execute arbitrary code remotely available from the application. This is usually accomplished through an insecurely configured PHP runtime environment ...

- XSS Using Alternate Syntax
Impact Scores: Financial: 1, Safety: 1, Privacy: 4.8
Risk Scores: Financial: 2.4, Safety: 2.4, Privacy: 11.52
Risk Factors: exposure: 0.60, complexity: 0.60, attack_surface: 0.20
Description: An adversary uses alternate forms of keywords or commands that result in the same action as the primary form but which may not be caught by filters. For example, many keywords are processed in a case ...

- Serialized Data External Linking
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.8
  Risk Scores: Financial: 2.4, Safety: 2.4, Privacy: 11.52
  Risk Factors: exposure: 0.60, complexity: 0.60, attack_surface: 0.20
  Description: An adversary creates a serialized data file (e.g. XML, YAML, etc...) that contains an external data reference. Because serialized data parsers may not validate documents with external references, ther...

- Leveraging Race Conditions
  Impact Scores: Financial: 4.8, Safety: 1, Privacy: 1
  Risk Scores: Financial: 11.52, Safety: 2.4, Privacy: 2.4
  Risk Factors: exposure: 0.60, complexity: 0.60, attack_surface: 0.20
  Description: The adversary targets a race condition occurring when multiple processes access and manipulate the same resource concurrently, and the outcome of the execution depends on the particular order in which...

- Leveraging Time-of-Check and Time-of-Use (TOCTOU) Race Conditions
  Impact Scores: Financial: 4.8, Safety: 1, Privacy: 1
  Risk Scores: Financial: 11.52, Safety: 2.4, Privacy: 2.4
  Risk Factors: exposure: 0.60, complexity: 0.60, attack_surface: 0.20
  Description: This attack targets a race condition occurring between the time of check (state) for a resource and the time of use of a resource. A typical example is file access. The adversary can leverage a file a...

- Using Meta-characters in E-mail Headers to Inject Malicious Payloads
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.8
  Risk Scores: Financial: 2.4, Safety: 2.4, Privacy: 11.52
  Risk Factors: exposure: 0.60, complexity: 0.60, attack_surface: 0.20
  Description: This type of attack involves an attacker leveraging meta-characters in email headers to inject improper behavior into email programs. Email software has become increasingly sophisticated and feature-r...

- Buffer Overflow via Symbolic Links
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.8
  Risk Scores: Financial: 2.4, Safety: 2.4, Privacy: 11.52
  Risk Factors: exposure: 0.60, complexity: 0.60, attack_surface: 0.20
  Description: This type of attack leverages the use of symbolic links to cause buffer overflows. An adversary can try to create or manipulate a symbolic link file such that its contents result in out of bounds data...

- Passing Local Filenames to Functions That Expect a URL
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.8
  Risk Scores: Financial: 2.4, Safety: 2.4, Privacy: 11.52
  Risk Factors: exposure: 0.60, complexity: 0.60, attack_surface: 0.20
  Description: This attack relies on client side code to access local files and resources instead of URLs. When the client browser is expecting a URL string, but instead receives a request for a local file, that exe...

- Session Credential Falsification through Prediction
  Impact Scores: Financial: 4.8, Safety: 1, Privacy: 1
  Risk Scores: Financial: 11.52, Safety: 2.4, Privacy: 2.4
  Risk Factors: exposure: 0.60, complexity: 0.60, attack_surface: 0.20
  Description: This attack targets predictable session ID in order to gain privileges. The attacker can predict the session ID used during a transaction to perform spoofing and session hijacking....

- Using Slashes and URL Encoding Combined to Bypass Validation Logic
  Impact Scores: Financial: 4.8, Safety: 1, Privacy: 1
  Risk Scores: Financial: 11.52, Safety: 2.4, Privacy: 2.4
  Risk Factors: exposure: 0.60, complexity: 0.60, attack_surface: 0.20

Description: This attack targets the encoding of the URL combined with the encoding of the slash characters. An attacker can take advantage of the multiple ways of encoding a URL and abuse the interpretation of th...

- Voice Phishing
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.8
  Risk Scores: Financial: 2.4, Safety: 2.4, Privacy: 11.52
  Risk Factors: exposure: 0.60, complexity: 0.60, attack_surface: 0.20
  Description: An adversary targets users with a phishing attack for the purpose of soliciting account passwords or sensitive information from the user. Voice Phishing is a variation of the Phishing social engineeri...

- Malicious Automated Software Update via Spoofing
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.8
  Risk Scores: Financial: 2.4, Safety: 2.4, Privacy: 11.52
  Risk Factors: exposure: 0.60, complexity: 0.60, attack_surface: 0.20
  Description: An attackers uses identify or content spoofing to trick a client into performing an automated software update from a malicious source. A malicious automated software update that leverages spoofing can...

- Blind SQL Injection
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.8
  Risk Scores: Financial: 2.4, Safety: 2.4, Privacy: 11.52
  Risk Factors: exposure: 0.60, complexity: 0.60, attack_surface: 0.20
  Description: Blind SQL Injection results from an insufficient mitigation for SQL Injection. Although suppressing database error messages are considered best practice, the suppression alone is not sufficient to pre...

- URL Encoding
  Impact Scores: Financial: 4.8, Safety: 1, Privacy: 1
  Risk Scores: Financial: 11.52, Safety: 2.4, Privacy: 2.4
  Risk Factors: exposure: 0.60, complexity: 0.60, attack_surface: 0.20
  Description: This attack targets the encoding of the URL. An adversary can take advantage of the multiple way of encoding an URL and abuse the interpretation of the URL....

- User-Controlled Filename
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.8
  Risk Scores: Financial: 2.4, Safety: 2.4, Privacy: 11.52
  Risk Factors: exposure: 0.60, complexity: 0.60, attack_surface: 0.20
  Description: An attack of this type involves an adversary inserting malicious characters (such as a XSS redirection) into a filename, directly or indirectly that is then used by the target software to generate HTM...

- Using Escaped Slashes in Alternate Encoding
  Impact Scores: Financial: 4.8, Safety: 1, Privacy: 1
  Risk Scores: Financial: 11.52, Safety: 2.4, Privacy: 2.4
  Risk Factors: exposure: 0.60, complexity: 0.60, attack_surface: 0.20
  Description: This attack targets the use of the backslash in alternate encoding. An adversary can provide a backslash as a leading character and causes a parser to believe that the next character is special. This ...

- Buffer Overflow in an API Call
  Impact Scores: Financial: 4.8, Safety: 1, Privacy: 1
  Risk Scores: Financial: 11.52, Safety: 2.4, Privacy: 2.4
  Risk Factors: exposure: 0.60, complexity: 0.60, attack_surface: 0.20
  Description: This attack targets libraries or shared code modules which are vulnerable to buffer overflow attacks. An adversary who has knowledge of known vulnerable libraries or shared code can easily target soft...

- Using UTF-8 Encoding to Bypass Validation Logic

Impact Scores: Financial: 1, Safety: 4.8, Privacy: 1
Risk Scores: Financial: 2.4, Safety: 11.52, Privacy: 2.4
Risk Factors: exposure: 0.60, complexity: 0.60, attack_surface: 0.20
Description: This attack is a specific variation on leveraging alternate encodings to bypass validation logic. This attack leverages the possibility to encode potentially harmful input in UTF-8 and submit it to ap...

- XPath Injection
Impact Scores: Financial: 1, Safety: 1, Privacy: 4.8
Risk Scores: Financial: 2.4, Safety: 2.4, Privacy: 11.52
Risk Factors: exposure: 0.60, complexity: 0.60, attack_surface: 0.20
Description: An attacker can craft special user-controllable input consisting of XPath expressions to inject the XML database and bypass authentication or glean information that they normally would not be able to....

- OS Command Injection
Impact Scores: Financial: 4.8, Safety: 1, Privacy: 1
Risk Scores: Financial: 11.52, Safety: 2.4, Privacy: 2.4
Risk Factors: exposure: 0.60, complexity: 0.60, attack_surface: 0.20
Description: In this type of an attack, an adversary injects operating system commands into existing application functions. An application that uses untrusted input to build command strings is vulnerable. An adver...

- Buffer Overflow in Local Command-Line Utilities
Impact Scores: Financial: 4.8, Safety: 1, Privacy: 1
Risk Scores: Financial: 11.52, Safety: 2.4, Privacy: 2.4
Risk Factors: exposure: 0.60, complexity: 0.60, attack_surface: 0.20
Description: This attack targets command-line utilities available in a number of shells. An adversary can leverage a vulnerability found in a command-line utility to escalate privilege to root....

- Reflection Attack in Authentication Protocol
Impact Scores: Financial: 1, Safety: 1, Privacy: 4.8
Risk Scores: Financial: 2.4, Safety: 2.4, Privacy: 11.52
Risk Factors: exposure: 0.60, complexity: 0.60, attack_surface: 0.20
Description: An adversary can abuse an authentication protocol susceptible to reflection attack in order to defeat it. Doing so allows the adversary illegitimate access to the target system, without possessing the...

- Forced Integer Overflow
Impact Scores: Financial: 1, Safety: 1, Privacy: 4.8
Risk Scores: Financial: 2.4, Safety: 2.4, Privacy: 11.52
Risk Factors: exposure: 0.60, complexity: 0.60, attack_surface: 0.20
Description: This attack forces an integer variable to go out of range. The integer variable is often used as an offset such as size of memory allocation or similarly. The attacker would typically control the valu...

- WSDL Scanning
Impact Scores: Financial: 1, Safety: 1, Privacy: 4.8
Risk Scores: Financial: 2.4, Safety: 2.4, Privacy: 11.52
Risk Factors: exposure: 0.60, complexity: 0.60, attack_surface: 0.20
Description: This attack targets the WSDL interface made available by a web service. The attacker may scan the WSDL interface to reveal sensitive information about invocation patterns, underlying technology implem...

- Root/Jailbreak Detection Evasion via Debugging
Impact Scores: Financial: 1, Safety: 1, Privacy: 5
Risk Scores: Financial: 1.7999999999999998, Safety: 1.7999999999999998, Privacy: 9.0
Risk Factors: exposure: 0.60, complexity: 0.60, attack_surface: 0.20
Description: An adversary inserts a debugger into the program entry point of a mobile application to modify the

application binary, with the goal of evading Root/Jailbreak detection. Mobile device users often Root...

- CAN Injection
  Impact Scores: Financial: 3.5999999999999996, Safety: 4.8, Privacy: 2.4
  Risk Scores: Financial: 6.479999999999999, Safety: 8.639999999999999, Privacy: 4.319999999999999
  Risk Factors: exposure: 0.60, complexity: 0.60, attack_surface: 0.20
  Description: Manipulation of CAN bus messages leading to vehicle malfunction...

- HTTP Request Splitting
  Impact Scores: Financial: 4.8, Safety: 1, Privacy: 1
  Risk Scores: Financial: 8.639999999999999, Safety: 1.7999999999999998, Privacy: 1.7999999999999998
  Risk Factors: exposure: 0.60, complexity: 0.60, attack_surface: 0.20
  Description: An adversary abuses the flexibility and discrepancies in the parsing and interpretation of HTTP Request messages by different intermediary HTTP agents (e.g., load balancer, reverse proxy, web caching ...

- Flooding
  Impact Scores: Financial: 1, Safety: 1.2, Privacy: 3.5999999999999996
  Risk Scores: Financial: 2.4, Safety: 2.88, Privacy: 8.639999999999999
  Risk Factors: exposure: 0.60, complexity: 0.60, attack_surface: 0.20
  Description: An adversary consumes the resources of a target by rapidly engaging in a large number of interactions with the target. This type of attack generally exposes a weakness in rate limiting or flow. When s...

- Directory Indexing
  Impact Scores: Financial: 1, Safety: 1, Privacy: 3.5999999999999996
  Risk Scores: Financial: 2.4, Safety: 2.4, Privacy: 8.639999999999999
  Risk Factors: exposure: 0.60, complexity: 0.60, attack_surface: 0.20
  Description: An adversary crafts a request to a target that results in the target listing/indexing the content of a directory as output. One common method of triggering directory contents as output is to construct...

- Flash Parameter Injection
  Impact Scores: Financial: 1, Safety: 1, Privacy: 3.5999999999999996
  Risk Scores: Financial: 2.4, Safety: 2.4, Privacy: 8.639999999999999
  Risk Factors: exposure: 0.60, complexity: 0.60, attack_surface: 0.20
  Description: An adversary takes advantage of improper data validation to inject malicious global parameters into a Flash file embedded within an HTML document. Flash files can leverage user-submitted data to confi...

- Exploiting Incorrectly Configured Access Control Security Levels
  Impact Scores: Financial: 1, Safety: 1, Privacy: 3.5999999999999996
  Risk Scores: Financial: 2.4, Safety: 2.4, Privacy: 8.639999999999999
  Risk Factors: exposure: 0.60, complexity: 0.60, attack_surface: 0.20
  Description: An attacker exploits a weakness in the configuration of access controls and is able to bypass the intended protection that these measures guard against and thereby obtain unauthorized access to the sy...

- Exponential Data Expansion
  Impact Scores: Financial: 1, Safety: 1, Privacy: 3.5999999999999996
  Risk Scores: Financial: 2.4, Safety: 2.4, Privacy: 8.639999999999999
  Risk Factors: exposure: 0.60, complexity: 0.60, attack_surface: 0.20
  Description: An adversary submits data to a target application which contains nested exponential data expansion to produce excessively large output. Many data format languages allow the definition of macro-like st...

- Inducing Account Lockout
  Impact Scores: Financial: 1, Safety: 1, Privacy: 3.5999999999999996
  Risk Scores: Financial: 2.4, Safety: 2.4, Privacy: 8.639999999999999

Risk Factors: exposure: 0.60, complexity: 0.60, attack_surface: 0.20
Description: An attacker leverages the security functionality of the system aimed at thwarting potential attacks to launch a denial of service attack against a legitimate system user. Many systems, for instance, i...

- XML Routing Detour Attacks
  Impact Scores: Financial: 1, Safety: 1, Privacy: 3.5999999999999996
  Risk Scores: Financial: 2.4, Safety: 2.4, Privacy: 8.639999999999999
  Risk Factors: exposure: 0.60, complexity: 0.60, attack_surface: 0.20
  Description: An attacker subverts an intermediate system used to process XML content and forces the intermediate to modify and/or re-route the processing of the content. XML Routing Detour Attacks are Adversary in...

- Serialized Data with Nested Payloads
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.8
  Risk Scores: Financial: 1.7999999999999998, Safety: 1.7999999999999998, Privacy: 8.639999999999999
  Risk Factors: exposure: 0.60, complexity: 0.60, attack_surface: 0.20
  Description: Applications often need to transform data in and out of a data format (e.g., XML and YAML) by using a parser. It may be possible for an adversary to inject data that may have an adverse effect on the ...

- Command Injection
  Impact Scores: Financial: 4.8, Safety: 1, Privacy: 1
  Risk Scores: Financial: 8.639999999999999, Safety: 1.7999999999999998, Privacy: 1.7999999999999998
  Risk Factors: exposure: 0.60, complexity: 0.60, attack_surface: 0.20
  Description: An adversary looking to execute a command of their choosing, injects new items into an existing command thus modifying interpretation away from what was intended. Commands in this context are often st...

- Leveraging Race Conditions via Symbolic Links
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.8
  Risk Scores: Financial: 1.7999999999999998, Safety: 1.7999999999999998, Privacy: 8.639999999999999
  Risk Factors: exposure: 0.60, complexity: 0.60, attack_surface: 0.20
  Description: This attack leverages the use of symbolic links (Symlinks) in order to write to sensitive files. An attacker can create a Symlink link to a target file not otherwise accessible to them. When the privi...

- HTTP Response Smuggling
  Impact Scores: Financial: 4.8, Safety: 1, Privacy: 1
  Risk Scores: Financial: 8.639999999999999, Safety: 1.7999999999999998, Privacy: 1.7999999999999998
  Risk Factors: exposure: 0.60, complexity: 0.60, attack_surface: 0.20
  Description: An adversary manipulates and injects malicious content in the form of secret unauthorized HTTP responses, into a single HTTP response from a vulnerable or compromised back-end HTTP agent (e.g., server...

- SOAP Manipulation
  Impact Scores: Financial: 4.8, Safety: 1, Privacy: 1
  Risk Scores: Financial: 8.639999999999999, Safety: 1.7999999999999998, Privacy: 1.7999999999999998
  Risk Factors: exposure: 0.60, complexity: 0.60, attack_surface: 0.20
  Description: Simple Object Access Protocol (SOAP) is used as a communication protocol between a client and server to invoke web services on the server. It is an XML-based protocol, and therefore suffers from many ...

- Fuzzing
  Impact Scores: Financial: 1, Safety: 1, Privacy: 3.5999999999999996
  Risk Scores: Financial: 2.4, Safety: 2.4, Privacy: 8.639999999999999
  Risk Factors: exposure: 0.60, complexity: 0.60, attack_surface: 0.20
  Description: In this attack pattern, the adversary leverages fuzzing to try to identify weaknesses in the system. Fuzzing is a software security and functionality testing method that feeds randomly constructed inp...

- HTTP Request Smuggling
  Impact Scores: Financial: 4.8, Safety: 1, Privacy: 1
  Risk Scores: Financial: 8.639999999999999, Safety: 1.7999999999999998, Privacy: 1.7999999999999998
  Risk Factors: exposure: 0.60, complexity: 0.60, attack_surface: 0.20
  Description: An adversary abuses the flexibility and discrepancies in the parsing and interpretation of HTTP Request messages using various HTTP headers, request-line and body parameters as well as message sizes (...

- HTTP Response Splitting
  Impact Scores: Financial: 4.8, Safety: 1, Privacy: 1
  Risk Scores: Financial: 8.639999999999999, Safety: 1.7999999999999998, Privacy: 1.7999999999999998
  Risk Factors: exposure: 0.60, complexity: 0.60, attack_surface: 0.20
  Description: An adversary manipulates and injects malicious content, in the form of secret unauthorized HTTP responses, into a single HTTP response from a vulnerable or compromised back-end HTTP agent (e.g., web s...

- Manipulating Opaque Client-based Data Tokens
  Impact Scores: Financial: 1, Safety: 1, Privacy: 3.5999999999999996
  Risk Scores: Financial: 2.4, Safety: 2.4, Privacy: 8.639999999999999
  Risk Factors: exposure: 0.60, complexity: 0.60, attack_surface: 0.20
  Description: In circumstances where an application holds important data client-side in tokens (cookies, URLs, data files, and so forth) that data can be manipulated. If client or server-side application components...

- Using Alternative IP Address Encodings
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.8
  Risk Scores: Financial: 1.7999999999999998, Safety: 1.7999999999999998, Privacy: 8.639999999999999
  Risk Factors: exposure: 0.60, complexity: 0.60, attack_surface: 0.20
  Description: This attack relies on the adversary using unexpected formats for representing IP addresses. Networked applications may expect network location information in a specific format, such as fully qualified...

- Exploiting Multiple Input Interpretation Layers
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.8
  Risk Scores: Financial: 1.7999999999999998, Safety: 1.7999999999999998, Privacy: 8.639999999999999
  Risk Factors: exposure: 0.60, complexity: 0.60, attack_surface: 0.20
  Description: An attacker supplies the target software with input data that contains sequences of special characters designed to bypass input validation logic. This exploit relies on the target making multiples pas...

- Development Alteration
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.8
  Risk Scores: Financial: 1.7999999999999998, Safety: 1.7999999999999998, Privacy: 8.639999999999999
  Risk Factors: exposure: 0.60, complexity: 0.60, attack_surface: 0.20
  Description: An adversary modifies a technology, product, or component during its development to acheive a negative impact once the system is deployed. The goal of the adversary is to modify the system in such a w...

- Malicious Logic Insertion into Product Software via Configuration Management Manipulation
  Impact Scores: Financial: 4.8, Safety: 1, Privacy: 1
  Risk Scores: Financial: 8.639999999999999, Safety: 1.7999999999999998, Privacy: 1.7999999999999998
  Risk Factors: exposure: 0.60, complexity: 0.60, attack_surface: 0.20
  Description: An adversary exploits a configuration management system so that malicious logic is inserted into a software products build, update or deployed environment. If an adversary can control the elements inc...

- Design Alteration
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.8
  Risk Scores: Financial: 1.7999999999999998, Safety: 1.7999999999999998, Privacy: 8.639999999999999
  Risk Factors: exposure: 0.60, complexity: 0.60, attack_surface: 0.20

Description: An adversary modifies the design of a technology, product, or component to acheive a negative impact once the system is deployed. In this type of attack, the goal of the adversary is to modify the des...

- Contradictory Destinations in Traffic Routing Schemes
  Impact Scores: Financial: 4.8, Safety: 1, Privacy: 1
  Risk Scores: Financial: 8.639999999999999, Safety: 1.7999999999999998, Privacy: 1.7999999999999998
  Risk Factors: exposure: 0.60, complexity: 0.60, attack_surface: 0.20
  Description: Adversaries can provide contradictory destinations when sending messages. Traffic is routed in networks using the domain names in various headers available at different levels of the OSI model. In a C...

- Object Injection
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.8
  Risk Scores: Financial: 1.7999999999999998, Safety: 1.7999999999999998, Privacy: 8.639999999999999
  Risk Factors: exposure: 0.60, complexity: 0.60, attack_surface: 0.20
  Description: An adversary attempts to exploit an application by injecting additional, malicious content during its processing of serialized objects. Developers leverage serialization in order to convert data or st...

- Bluetooth Impersonation AttackS (BIAS)
  Impact Scores: Financial: 4.8, Safety: 1, Privacy: 1
  Risk Scores: Financial: 8.639999999999999, Safety: 1.7999999999999998, Privacy: 1.7999999999999998
  Risk Factors: exposure: 0.60, complexity: 0.60, attack_surface: 0.20
  Description: An adversary disguises the MAC address of their Bluetooth enabled device to one for which there exists an active and trusted connection and authenticates successfully. The adversary can then perform m...

- Alteration of a Software Update
  Impact Scores: Financial: 4.8, Safety: 1, Privacy: 1
  Risk Scores: Financial: 8.639999999999999, Safety: 1.7999999999999998, Privacy: 1.7999999999999998
  Risk Factors: exposure: 0.60, complexity: 0.60, attack_surface: 0.20
  Description: An adversary with access to an organization’s software update infrastructure inserts malware into the content of an outgoing update to fielded systems where a wide range of malicious effects are possi...

- Eavesdropping on a Monitor
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.8
  Risk Scores: Financial: 1.7999999999999998, Safety: 1.7999999999999998, Privacy: 8.639999999999999
  Risk Factors: exposure: 0.60, complexity: 0.60, attack_surface: 0.20
  Description: An Adversary can eavesdrop on the content of an external monitor through the air without modifying any cable or installing software, just capturing this signal emitted by the cable or video port, with...

- Network Boundary Bridging
  Impact Scores: Financial: 4.8, Safety: 1, Privacy: 1
  Risk Scores: Financial: 8.639999999999999, Safety: 1.7999999999999998, Privacy: 1.7999999999999998
  Risk Factors: exposure: 0.60, complexity: 0.60, attack_surface: 0.20
  Description: An adversary which has gained elevated access to network boundary devices may use these devices to create a channel to bridge trusted and untrusted networks. Boundary devices do not necessarily have t...

- Browser in the Middle (BiTM)
  Impact Scores: Financial: 4.8, Safety: 1, Privacy: 1
  Risk Scores: Financial: 8.639999999999999, Safety: 1.7999999999999998, Privacy: 1.7999999999999998
  Risk Factors: exposure: 0.60, complexity: 0.60, attack_surface: 0.20
  Description: An adversary exploits the inherent functionalities of a web browser, in order to establish an unnoticed remote desktop connection in the victim's browser to the adversary's system. The adversary must ...

- Manipulating State

  Impact Scores: Financial: 1.2, Safety: 1, Privacy: 4.8
  Risk Scores: Financial: 2.1599999999999997, Safety: 1.7999999999999998, Privacy: 8.639999999999999
  Risk Factors: exposure: 0.60, complexity: 0.60, attack_surface: 0.20
  Description: The adversary modifies state information maintained by the target software or causes a state transition in hardware. If successful, the target will use this tainted state and execute in an unintended ...

- Interface Manipulation
  Impact Scores: Financial: 3.5999999999999996, Safety: 1, Privacy: 1
  Risk Scores: Financial: 6.479999999999999, Safety: 1.7999999999999998, Privacy: 1.7999999999999998
  Risk Factors: exposure: 0.60, complexity: 0.60, attack_surface: 0.20
  Description: An adversary manipulates the use or processing of an interface (e.g. Application Programming Interface (API) or System-on-Chip (SoC)) resulting in an adverse impact upon the security of the system imp...

- Parameter Injection
  Impact Scores: Financial: 1, Safety: 1, Privacy: 3.5999999999999996
  Risk Scores: Financial: 1.7999999999999998, Safety: 1.7999999999999998, Privacy: 6.479999999999999
  Risk Factors: exposure: 0.60, complexity: 0.60, attack_surface: 0.20
  Description: An adversary manipulates the content of request parameters for the purpose of undermining the security of the target. Some parameter encodings use text characters as separators. For example, parameter...

- Content Spoofing
  Impact Scores: Financial: 3.5999999999999996, Safety: 1, Privacy: 3.5999999999999996
  Risk Scores: Financial: 6.479999999999999, Safety: 1.7999999999999998, Privacy: 6.479999999999999
  Risk Factors: exposure: 0.60, complexity: 0.60, attack_surface: 0.20
  Description: An adversary modifies content to make it contain something other than what the original content producer intended while keeping the apparent source of the content unchanged. The term content spoofing ...

- Resource Location Spoofing
  Impact Scores: Financial: 1, Safety: 1, Privacy: 3.5999999999999996
  Risk Scores: Financial: 1.7999999999999998, Safety: 1.7999999999999998, Privacy: 6.479999999999999
  Risk Factors: exposure: 0.60, complexity: 0.60, attack_surface: 0.20
  Description: An adversary deceives an application or user and convinces them to request a resource from an unintended location. By spoofing the location, the adversary can cause an alternate resource to be used, o...

- Cross-Site Flashing
  Impact Scores: Financial: 3.5999999999999996, Safety: 1, Privacy: 1
  Risk Scores: Financial: 6.479999999999999, Safety: 1.7999999999999998, Privacy: 1.7999999999999998
  Risk Factors: exposure: 0.60, complexity: 0.60, attack_surface: 0.20
  Description: An attacker is able to trick the victim into executing a Flash document that passes commands or calls to a Flash player browser plugin, allowing the attacker to exploit native Flash functionality in t...

- Modification of Registry Run Keys
  Impact Scores: Financial: 1, Safety: 1, Privacy: 3.5999999999999996
  Risk Scores: Financial: 1.7999999999999998, Safety: 1.7999999999999998, Privacy: 6.479999999999999
  Risk Factors: exposure: 0.60, complexity: 0.60, attack_surface: 0.20
  Description: An adversary adds a new entry to the run keys in the Windows registry so that an application of their choosing is executed when a user logs in. In this way, the adversary can get their executable to o...

- Using Leading 'Ghost' Character Sequences to Bypass Input Filters
  Impact Scores: Financial: 1, Safety: 1, Privacy: 3.5999999999999996
  Risk Scores: Financial: 1.7999999999999998, Safety: 1.7999999999999998, Privacy: 6.479999999999999
  Risk Factors: exposure: 0.60, complexity: 0.60, attack_surface: 0.20
  Description: Some APIs will strip certain leading characters from a string of parameters. An adversary can intentionally

introduce leading ghost characters (extra characters that don't affect the validity of the r...

- Manipulate Human Behavior
  Impact Scores: Financial: 1, Safety: 1, Privacy: 3.5999999999999996
  Risk Scores: Financial: 1.7999999999999998, Safety: 1.7999999999999998, Privacy: 6.479999999999999
  Risk Factors: exposure: 0.60, complexity: 0.60, attack_surface: 0.20
  Description: An adversary exploits inherent human psychological predisposition to influence a targeted individual or group to solicit information or manipulate the target into performing an action that serves the ...

- Disable Security Software
  Impact Scores: Financial: 3.5999999999999996, Safety: 1, Privacy: 1
  Risk Scores: Financial: 6.479999999999999, Safety: 1.7999999999999998, Privacy: 1.7999999999999998
  Risk Factors: exposure: 0.60, complexity: 0.60, attack_surface: 0.20
  Description: An adversary exploits a weakness in access control to disable security tools so that detection does not occur. This can take the form of killing processes, deleting registry keys so that tools do not ...

- Collect Data from Registries
  Impact Scores: Financial: 1, Safety: 1, Privacy: 3.5999999999999996
  Risk Scores: Financial: 1.7999999999999998, Safety: 1.7999999999999998, Privacy: 6.479999999999999
  Risk Factors: exposure: 0.60, complexity: 0.60, attack_surface: 0.20
  Description: An adversary exploits a weakness in authorization to gather system-specific data and sensitive information within a registry (e.g., Windows Registry, Mac plist). These contain information about the sy...

- Collect Data from Screen Capture
  Impact Scores: Financial: 1, Safety: 1, Privacy: 3.5999999999999996
  Risk Scores: Financial: 1.7999999999999998, Safety: 1.7999999999999998, Privacy: 6.479999999999999
  Risk Factors: exposure: 0.60, complexity: 0.60, attack_surface: 0.20
  Description: An adversary gathers sensitive information by exploiting the system's screen capture functionality. Through screenshots, the adversary aims to see what happens on the screen over the course of an oper...

- Retrieve Data from Decommissioned Devices
  Impact Scores: Financial: 1, Safety: 1.2, Privacy: 3.5999999999999996
  Risk Scores: Financial: 1.7999999999999998, Safety: 2.1599999999999997, Privacy: 6.479999999999999
  Risk Factors: exposure: 0.60, complexity: 0.60, attack_surface: 0.20
  Description: An adversary obtains decommissioned, recycled, or discarded systems and devices that can include an organization’s intellectual property, employee data, and other types of controlled information. Syst...

- Escaping a Sandbox by Calling Code in Another Language
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5
  Risk Scores: Financial: 1.2, Safety: 1.2, Privacy: 6.0
  Risk Factors: exposure: 0.60, complexity: 0.60, attack_surface: 0.20
  Description: The attacker may submit malicious code of another language to obtain access to privileges that were not intentionally exposed by the sandbox, thus escaping the sandbox. For instance, Java code cannot ...

- Hijacking a Privileged Thread of Execution
  Impact Scores: Financial: 5, Safety: 1, Privacy: 1
  Risk Scores: Financial: 6.0, Safety: 1.2, Privacy: 1.2
  Risk Factors: exposure: 0.60, complexity: 0.60, attack_surface: 0.20
  Description: An adversary hijacks a privileged thread of execution by injecting malicious code into a running process. By using a privleged thread to do their bidding, adversaries can evade process-based detection...

- Subvert Code-signing Facilities
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5

Risk Scores: Financial: 1.2, Safety: 1.2, Privacy: 6.0
Risk Factors: exposure: 0.60, complexity: 0.60, attack_surface: 0.20
Description: Many languages use code signing facilities to vouch for code's identity and to thus tie code to its assigned privileges within an environment. Subverting this mechanism can be instrumental in an attac...

- Load Value Injection
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5
  Risk Scores: Financial: 1.2, Safety: 1.2, Privacy: 6.0
  Risk Factors: exposure: 0.60, complexity: 0.60, attack_surface: 0.20
  Description: An adversary exploits a hardware design flaw in a CPU implementation of transient instruction execution in which a faulting or assisted load instruction transiently forwards adversary-controlled data ...

- Web Application Fingerprinting
  Impact Scores: Financial: 1, Safety: 1, Privacy: 2.4
  Risk Scores: Financial: 2.4, Safety: 2.4, Privacy: 5.76
  Risk Factors: exposure: 0.60, complexity: 0.60, attack_surface: 0.20
  Description: An attacker sends a series of probes to a web application in order to elicit version-dependent and type-dependent behavior that assists in identifying the target. An attacker could learn information s...

- Fuzzing for application mapping
  Impact Scores: Financial: 1, Safety: 2.4, Privacy: 1
  Risk Scores: Financial: 2.4, Safety: 5.76, Privacy: 2.4
  Risk Factors: exposure: 0.60, complexity: 0.60, attack_surface: 0.20
  Description: An attacker sends random, malformed, or otherwise unexpected messages to a target application and observes the application's log or error messages returned. The attacker does not initially know how a ...

- Forced Deadlock
  Impact Scores: Financial: 4.8, Safety: 1, Privacy: 1
  Risk Scores: Financial: 5.76, Safety: 1.2, Privacy: 1.2
  Risk Factors: exposure: 0.60, complexity: 0.60, attack_surface: 0.20
  Description: The adversary triggers and exploits a deadlock condition in the target software to cause a denial of service. A deadlock can occur when two or more competing actions are waiting for each other to fini...

- Schema Poisoning
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.8
  Risk Scores: Financial: 1.2, Safety: 1.2, Privacy: 5.76
  Risk Factors: exposure: 0.60, complexity: 0.60, attack_surface: 0.20
  Description: An adversary corrupts or modifies the content of a schema for the purpose of undermining the security of the target. Schemas provide the structure and content definitions for resources used by an appl...

- USB Memory Attacks
  Impact Scores: Financial: 2.4, Safety: 1, Privacy: 4.8
  Risk Scores: Financial: 2.88, Safety: 1.2, Privacy: 5.76
  Risk Factors: exposure: 0.60, complexity: 0.60, attack_surface: 0.20
  Description: An adversary loads malicious code onto a USB memory stick in order to infect any system which the device is plugged in to. USB drives present a significant security risk for business and government ag...

- Signature Spoofing by Misrepresentation
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.8
  Risk Scores: Financial: 1.2, Safety: 1.2, Privacy: 5.76
  Risk Factors: exposure: 0.60, complexity: 0.60, attack_surface: 0.20
  Description: An attacker exploits a weakness in the parsing or display code of the recipient software to generate a data blob containing a supposedly valid signature, but the signer's identity is falsely represent...

- Hardware Component Substitution During Baselining
  Impact Scores: Financial: 4.8, Safety: 1, Privacy: 1
  Risk Scores: Financial: 5.76, Safety: 1.2, Privacy: 1.2
  Risk Factors: exposure: 0.60, complexity: 0.60, attack_surface: 0.20
  Description: An adversary with access to system components during allocated baseline development can substitute a maliciously altered hardware component for a baseline component during the product development and ...

- Malicious Hardware Update
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.8
  Risk Scores: Financial: 1.2, Safety: 1.2, Privacy: 5.76
  Risk Factors: exposure: 0.60, complexity: 0.60, attack_surface: 0.20
  Description: An adversary introduces malicious hardware during an update or replacement procedure, allowing for additional compromise or site disruption at the victim location. After deployment, it is not uncommon...

- Open-Source Library Manipulation
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.8
  Risk Scores: Financial: 1.2, Safety: 1.2, Privacy: 5.76
  Risk Factors: exposure: 0.60, complexity: 0.60, attack_surface: 0.20
  Description: Adversaries implant malicious code in open source software (OSS) libraries to have it widely distributed, as OSS is commonly downloaded by developers and other users to incorporate into software devel...

- ASIC With Malicious Functionality
  Impact Scores: Financial: 4.8, Safety: 1, Privacy: 1
  Risk Scores: Financial: 5.76, Safety: 1.2, Privacy: 1.2
  Risk Factors: exposure: 0.60, complexity: 0.60, attack_surface: 0.20
  Description: An attacker with access to the development environment process of an application-specific integrated circuit (ASIC) for a victim system being developed or maintained after initial deployment can inser...

- Hardware Fault Injection
  Impact Scores: Financial: 1, Safety: 4.8, Privacy: 4.8
  Risk Scores: Financial: 1.2, Safety: 5.76, Privacy: 5.76
  Risk Factors: exposure: 0.60, complexity: 0.60, attack_surface: 0.20
  Description: The adversary uses disruptive signals or events, or alters the physical environment a device operates in, to cause faulty behavior in electronic devices. This can include electromagnetic pulses, laser...

- Carry-Off GPS Attack
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.8
  Risk Scores: Financial: 1.2, Safety: 1.2, Privacy: 5.76
  Risk Factors: exposure: 0.60, complexity: 0.60, attack_surface: 0.20
  Description: A common form of a GPS spoofing attack, commonly termed a carry-off attack begins with an adversary broadcasting signals synchronized with the genuine signals observed by the target receiver. The powe...

- DLL Side-Loading
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.8
  Risk Scores: Financial: 1.2, Safety: 1.2, Privacy: 5.76
  Risk Factors: exposure: 0.60, complexity: 0.60, attack_surface: 0.20
  Description: An adversary places a malicious version of a Dynamic-Link Library (DLL) in the Windows Side-by-Side (WinSxS) directory to trick the operating system into loading this malicious DLL instead of a legiti...

- Use of Captured Tickets (Pass The Ticket)
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.8
  Risk Scores: Financial: 1.2, Safety: 1.2, Privacy: 5.76
  Risk Factors: exposure: 0.60, complexity: 0.60, attack_surface: 0.20

Description: An adversary uses stolen Kerberos tickets to access systems/resources that leverage the Kerberos authentication protocol. The Kerberos authentication protocol centers around a ticketing system which i...

- Sniff Application Code
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.8
  Risk Scores: Financial: 1.2, Safety: 1.2, Privacy: 5.76
  Risk Factors: exposure: 0.60, complexity: 0.60, attack_surface: 0.20
  Description: An adversary passively sniffs network communications and captures application code bound for an authorized client. Once obtained, they can use it as-is, or through reverse-engineering glean sensitive ...

- Key Negotiation of Bluetooth Attack (KNOB)
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.8
  Risk Scores: Financial: 1.2, Safety: 1.2, Privacy: 5.76
  Risk Factors: exposure: 0.60, complexity: 0.60, attack_surface: 0.20
  Description: An adversary can exploit a flaw in Bluetooth key negotiation allowing them to decrypt information sent between two devices communicating via Bluetooth. The adversary uses an Adversary in the Middle se...

- Malicious Code Implanted During Chip Programming
  Impact Scores: Financial: 4.8, Safety: 1, Privacy: 1
  Risk Scores: Financial: 5.76, Safety: 1.2, Privacy: 1.2
  Risk Factors: exposure: 0.60, complexity: 0.60, attack_surface: 0.20
  Description: During the programming step of chip manufacture, an adversary with access and necessary technical skills maliciously alters a chip’s intended program logic to produce an effect intended by the adversa...

- AJAX Footprinting
  Impact Scores: Financial: 1, Safety: 1, Privacy: 2.4
  Risk Scores: Financial: 2.4, Safety: 2.4, Privacy: 5.76
  Risk Factors: exposure: 0.60, complexity: 0.60, attack_surface: 0.20
  Description: This attack utilizes the frequent client-server roundtrips in Ajax conversation to scan a system. While Ajax does not open up new vulnerabilities per se, it does optimize them from an attacker point o...

- Interception
  Impact Scores: Financial: 1, Safety: 1, Privacy: 3.5999999999999996
  Risk Scores: Financial: 1.2, Safety: 1.2, Privacy: 4.319999999999999
  Risk Factors: exposure: 0.60, complexity: 0.60, attack_surface: 0.20
  Description: An adversary monitors data streams to or from the target for information gathering purposes. This attack may be undertaken to solely gather sensitive information or to support a further attack against...

- XML Ping of the Death
  Impact Scores: Financial: 1, Safety: 3.5999999999999996, Privacy: 1
  Risk Scores: Financial: 1.2, Safety: 4.319999999999999, Privacy: 1.2
  Risk Factors: exposure: 0.60, complexity: 0.60, attack_surface: 0.20
  Description: An attacker initiates a resource depletion attack where a large number of small XML messages are delivered at a sufficiently rapid rate to cause a denial of service or crash of the target. Transaction...

- Active OS Fingerprinting
  Impact Scores: Financial: 1, Safety: 1, Privacy: 2.4
  Risk Scores: Financial: 1.7999999999999998, Safety: 1.7999999999999998, Privacy: 4.319999999999999
  Risk Factors: exposure: 0.60, complexity: 0.60, attack_surface: 0.20
  Description: An adversary engages in activity to detect the operating system or firmware version of a remote target by interrogating a device, server, or platform with a probe designed to solicit behavior that wil...

- TCP Timestamp Probe

Impact Scores: Financial: 2.4, Safety: 1, Privacy: 1
Risk Scores: Financial: 4.319999999999999, Safety: 1.7999999999999998, Privacy: 1.7999999999999998
Risk Factors: exposure: 0.60, complexity: 0.60, attack_surface: 0.20
Description: This OS fingerprinting probe examines the remote server's implementation of TCP timestamps. Not all operating systems implement timestamps within the TCP header, but when timestamps are used then this...

- TCP Sequence Number Probe
  Impact Scores: Financial: 2.4, Safety: 1, Privacy: 1
  Risk Scores: Financial: 4.319999999999999, Safety: 1.7999999999999998, Privacy: 1.7999999999999998
  Risk Factors: exposure: 0.60, complexity: 0.60, attack_surface: 0.20
  Description: This OS fingerprinting probe tests the target system's assignment of TCP sequence numbers. One common way to test TCP Sequence Number generation is to send a probe packet to an open port on the target...

- TCP (ISN) Greatest Common Divisor Probe
  Impact Scores: Financial: 1, Safety: 1, Privacy: 2.4
  Risk Scores: Financial: 1.7999999999999998, Safety: 1.7999999999999998, Privacy: 4.319999999999999
  Risk Factors: exposure: 0.60, complexity: 0.60, attack_surface: 0.20
  Description: This OS fingerprinting probe sends a number of TCP SYN packets to an open port of a remote machine. The Initial Sequence Number (ISN) in each of the SYN/ACK response packets is analyzed to determine t...

- TCP (ISN) Counter Rate Probe
  Impact Scores: Financial: 1, Safety: 1, Privacy: 2.4
  Risk Scores: Financial: 1.7999999999999998, Safety: 1.7999999999999998, Privacy: 4.319999999999999
  Risk Factors: exposure: 0.60, complexity: 0.60, attack_surface: 0.20
  Description: This OS detection probe measures the average rate of initial sequence number increments during a period of time. Sequence numbers are incremented using a time-based algorithm and are susceptible to a ...

- TCP (ISN) Sequence Predictability Probe
  Impact Scores: Financial: 1, Safety: 1, Privacy: 2.4
  Risk Scores: Financial: 1.7999999999999998, Safety: 1.7999999999999998, Privacy: 4.319999999999999
  Risk Factors: exposure: 0.60, complexity: 0.60, attack_surface: 0.20
  Description: This type of operating system probe attempts to determine an estimate for how predictable the sequence number generation algorithm is for a remote host. Statistical techniques, such as standard deviat...

- TCP Initial Window Size Probe
  Impact Scores: Financial: 2.4, Safety: 1, Privacy: 1
  Risk Scores: Financial: 4.319999999999999, Safety: 1.7999999999999998, Privacy: 1.7999999999999998
  Risk Factors: exposure: 0.60, complexity: 0.60, attack_surface: 0.20
  Description: This OS fingerprinting probe checks the initial TCP Window size. TCP stacks limit the range of sequence numbers allowable within a session to maintain the connected state within TCP protocol logic. Th...

- TCP Options Probe
  Impact Scores: Financial: 2.4, Safety: 1, Privacy: 1
  Risk Scores: Financial: 4.319999999999999, Safety: 1.7999999999999998, Privacy: 1.7999999999999998
  Risk Factors: exposure: 0.60, complexity: 0.60, attack_surface: 0.20
  Description: This OS fingerprinting probe analyzes the type and order of any TCP header options present within a response segment. Most operating systems use unique ordering and different option sets when options ...

- Pretexting
  Impact Scores: Financial: 1, Safety: 1, Privacy: 2.4
  Risk Scores: Financial: 1.7999999999999998, Safety: 1.7999999999999998, Privacy: 4.319999999999999
  Risk Factors: exposure: 0.60, complexity: 0.60, attack_surface: 0.20
  Description: An adversary engages in pretexting behavior to solicit information from target persons, or manipulate the

target into performing some action that serves the adversary's interests. During a pretexting ...

- Incomplete Data Deletion in a Multi-Tenant Environment
  Impact Scores: Financial: 1, Safety: 1, Privacy: 3.5999999999999996
  Risk Scores: Financial: 1.2, Safety: 1.2, Privacy: 4.319999999999999
  Risk Factors: exposure: 0.60, complexity: 0.60, attack_surface: 0.20
  Description: An adversary obtains unauthorized information due to insecure or incomplete data deletion in a multi-tenant environment. If a cloud provider fails to completely delete storage and data from former clo...

- Adding a Space to a File Extension
  Impact Scores: Financial: 1, Safety: 1, Privacy: 3.5999999999999996
  Risk Scores: Financial: 1.2, Safety: 1.2, Privacy: 4.319999999999999
  Risk Factors: exposure: 0.60, complexity: 0.60, attack_surface: 0.20
  Description: An adversary adds a space character to the end of a file extension and takes advantage of an application that does not properly neutralize trailing special elements in file names. This extra space, wh...

- Reverse Engineering
  Impact Scores: Financial: 2.4, Safety: 1, Privacy: 1
  Risk Scores: Financial: 2.88, Safety: 1.2, Privacy: 1.2
  Risk Factors: exposure: 0.60, complexity: 0.60, attack_surface: 0.20
  Description: An adversary discovers the structure, function, and composition of an object, resource, or system by using a variety of analysis techniques to effectively determine how the analyzed entity was constru...

- Fingerprinting
  Impact Scores: Financial: 1, Safety: 1, Privacy: 1.2
  Risk Scores: Financial: 2.4, Safety: 2.4, Privacy: 2.88
  Risk Factors: exposure: 0.60, complexity: 0.60, attack_surface: 0.20
  Description: An adversary compares output from a target system to known indicators that uniquely identify specific details about the target. Most commonly, fingerprinting is done to determine operating system and ...

- Target Influence via Framing
  Impact Scores: Financial: 1, Safety: 1.2, Privacy: 2.4
  Risk Scores: Financial: 1.2, Safety: 1.44, Privacy: 2.88
  Risk Factors: exposure: 0.60, complexity: 0.60, attack_surface: 0.20
  Description: An adversary uses framing techniques to contextualize a conversation so that the target is more likely to be influenced by the adversary's point of view. Framing is information and experiences in life...

- Influence via Psychological Principles
  Impact Scores: Financial: 2.4, Safety: 1, Privacy: 1
  Risk Scores: Financial: 2.88, Safety: 1.2, Privacy: 1.2
  Risk Factors: exposure: 0.60, complexity: 0.60, attack_surface: 0.20
  Description: The adversary shapes the target's actions or behavior by focusing on the ways human interact and learn, leveraging such elements as cognitive and social psychology. In a variety of ways, a target can ...

- Process Footprinting
  Impact Scores: Financial: 1, Safety: 1, Privacy: 2.4
  Risk Scores: Financial: 1.2, Safety: 1.2, Privacy: 2.88
  Risk Factors: exposure: 0.60, complexity: 0.60, attack_surface: 0.20
  Description: An adversary exploits functionality meant to identify information about the currently running processes on the target system to an authorized user. By knowing what processes are running on the target ...

- Services Footprinting
  Impact Scores: Financial: 1, Safety: 1, Privacy: 2.4

Risk Scores: Financial: 1.2, Safety: 1.2, Privacy: 2.88
Risk Factors: exposure: 0.60, complexity: 0.60, attack_surface: 0.20
Description: An adversary exploits functionality meant to identify information about the services on the target system to an authorized user. By knowing what services are registered on the target system, the adver...

- Account Footprinting
  Impact Scores: Financial: 1, Safety: 1, Privacy: 2.4
  Risk Scores: Financial: 1.2, Safety: 1.2, Privacy: 2.88
  Risk Factors: exposure: 0.60, complexity: 0.60, attack_surface: 0.20
  Description: An adversary exploits functionality meant to identify information about the domain accounts and their permissions on the target system to an authorized user. By knowing what accounts are registered on...

- Group Permission Footprinting
  Impact Scores: Financial: 1, Safety: 1, Privacy: 2.4
  Risk Scores: Financial: 1.2, Safety: 1.2, Privacy: 2.88
  Risk Factors: exposure: 0.60, complexity: 0.60, attack_surface: 0.20
  Description: An adversary exploits functionality meant to identify information about user groups and their permissions on the target system to an authorized user. By knowing what users/permissions are registered o...

- Owner Footprinting
  Impact Scores: Financial: 1, Safety: 1, Privacy: 2.4
  Risk Scores: Financial: 1.2, Safety: 1.2, Privacy: 2.88
  Risk Factors: exposure: 0.60, complexity: 0.60, attack_surface: 0.20
  Description: An adversary exploits functionality meant to identify information about the primary users on the target system to an authorized user. They may do this, for example, by reviewing logins or file modific...

- System Footprinting
  Impact Scores: Financial: 1, Safety: 1, Privacy: 2.4
  Risk Scores: Financial: 1.2, Safety: 1.2, Privacy: 2.88
  Risk Factors: exposure: 0.60, complexity: 0.60, attack_surface: 0.20
  Description: An adversary engages in active probing and exploration activities to determine security information about a remote target system. Often times adversaries will rely on remote applications that can be p...

- Collect Data from Clipboard
  Impact Scores: Financial: 1, Safety: 1, Privacy: 2.4
  Risk Scores: Financial: 1.2, Safety: 1.2, Privacy: 2.88
  Risk Factors: exposure: 0.60, complexity: 0.60, attack_surface: 0.20
  Description: The adversary exploits an application that allows for the copying of sensitive data or information by collecting information copied to the clipboard. Data copied to the clipboard can be accessed by ot...

Component: Electronic Throttle

Type: Actuator
Safety Level: ASIL C
Interfaces: CAN
Access Points:
Data Types: Control Commands
Location: Internal
Trust Zone: Critical
Connected To: ECU001

Identified Threats:

- Buffer Manipulation
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5
  Risk Scores: Financial: 2.24, Safety: 2.24, Privacy: 11.200000000000001
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: An adversary manipulates an application's interaction with a buffer in an attempt to read or modify data they shouldn't have access to. Buffer attacks are distinguished in that it is the buffer space ...

- Redirect Access to Libraries
  Impact Scores: Financial: 1, Safety: 5, Privacy: 1
  Risk Scores: Financial: 2.24, Safety: 11.200000000000001, Privacy: 2.24
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: An adversary exploits a weakness in the way an application searches for external libraries to manipulate the execution flow to point to an adversary supplied library or code base. This pattern of atta...

- XSS Targeting Non-Script Elements
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5
  Risk Scores: Financial: 2.24, Safety: 2.24, Privacy: 11.200000000000001
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: This attack is a form of Cross-Site Scripting (XSS) where malicious scripts are embedded in elements that are not expected to host scripts such as image tags (<img>), comments in XML documents (< !-CD...

- Retrieve Embedded Sensitive Data
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5
  Risk Scores: Financial: 2.24, Safety: 2.24, Privacy: 11.200000000000001
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: An attacker examines a target system to find sensitive data that has been embedded within it. This information can reveal confidential contents, such as account numbers or individual keys/credentials ...

- Leveraging/Manipulating Configuration File Search Paths
  Impact Scores: Financial: 5, Safety: 1, Privacy: 1
  Risk Scores: Financial: 11.200000000000001, Safety: 2.24, Privacy: 2.24
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: This pattern of attack sees an adversary load a malicious resource into a program's standard path so that when a known command is executed then the system instead executes the malicious component. The...

- Manipulating Writeable Terminal Devices
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5
  Risk Scores: Financial: 2.24, Safety: 2.24, Privacy: 11.200000000000001
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: This attack exploits terminal devices that allow themselves to be written to by other users. The attacker sends command strings to the target terminal device hoping that the target user will hit enter...

- Overflow Binary Resource File
  Impact Scores: Financial: 5, Safety: 1, Privacy: 1
  Risk Scores: Financial: 11.200000000000001, Safety: 2.24, Privacy: 2.24
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: An attack of this type exploits a buffer overflow vulnerability in the handling of binary resources. Binary resources may include music files like MP3, image files like JPEG files, and any other binar...

- Poison Web Service Registry
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5

Risk Scores: Financial: 2.24, Safety: 2.24, Privacy: 11.200000000000001
Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
Description: SOA and Web Services often use a registry to perform look up, get schema information, and metadata about services. A poisoned registry can redirect (think phishing for servers) the service requester t...

- String Format Overflow in syslog()
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5
  Risk Scores: Financial: 2.24, Safety: 2.24, Privacy: 11.200000000000001
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: This attack targets applications and software that uses the syslog() function insecurely. If an application does not explicitely use a format string parameter in a call to syslog(), user input can be ...

- Manipulating User-Controlled Variables
  Impact Scores: Financial: 2.4, Safety: 1, Privacy: 5
  Risk Scores: Financial: 5.376, Safety: 2.24, Privacy: 11.200000000000001
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: This attack targets user controlled variables (DEBUG=1, PHP Globals, and So Forth). An adversary can override variables leveraging user-supplied, untrusted query variables directly used on the applica...

- XQuery Injection
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5
  Risk Scores: Financial: 2.24, Safety: 2.24, Privacy: 11.200000000000001
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: This attack utilizes XQuery to probe and attack server systems; in a similar manner that SQL Injection allows an attacker to exploit SQL calls to RDBMS, XQuery Injection uses improperly validated data...

- Pharming
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5
  Risk Scores: Financial: 2.24, Safety: 2.24, Privacy: 11.200000000000001
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: A pharming attack occurs when the victim is fooled into entering sensitive data into supposedly trusted locations, such as an online bank site or a trading platform. An attacker can impersonate these ...

- Phishing
  Impact Scores: Financial: 1.2, Safety: 1, Privacy: 5
  Risk Scores: Financial: 2.688, Safety: 2.24, Privacy: 11.200000000000001
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: Phishing is a social engineering technique where an attacker masquerades as a legitimate entity with which the victim might do business in order to prompt the user to reveal some confidential informat...

- Accessing Functionality Not Properly Constrained by ACLs
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.8
  Risk Scores: Financial: 2.24, Safety: 2.24, Privacy: 10.752
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: In applications, particularly web applications, access to functionality is mitigated by an authorization framework. This framework maps Access Control Lists (ACLs) to elements of the application's fun...

- Buffer Overflow via Environment Variables
  Impact Scores: Financial: 4.8, Safety: 1, Privacy: 1
  Risk Scores: Financial: 10.752, Safety: 2.24, Privacy: 2.24
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: This attack pattern involves causing a buffer overflow through manipulation of environment variables. Once the adversary finds that they can modify an environment variable, they may try to overflow as...

- Server Side Include (SSI) Injection
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.8
  Risk Scores: Financial: 2.24, Safety: 2.24, Privacy: 10.752
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: An attacker can use Server Side Include (SSI) Injection to send code to a web application that then gets executed by the web server. Doing so enables the attacker to achieve similar results to Cross S...

- Format String Injection
  Impact Scores: Financial: 1, Safety: 2.4, Privacy: 4.8
  Risk Scores: Financial: 2.24, Safety: 5.376, Privacy: 10.752
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: An adversary includes formatting characters in a string input field on the target application. Most applications assume that users will provide static text and may respond unpredictably to the presenc...

- Cache Poisoning
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.8
  Risk Scores: Financial: 2.24, Safety: 2.24, Privacy: 10.752
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: An attacker exploits the functionality of cache technologies to cause specific data to be cached that aids the attackers' objectives. This describes any attack whereby an attacker places incorrect or ...

- DNS Cache Poisoning
  Impact Scores: Financial: 4.8, Safety: 1, Privacy: 1
  Risk Scores: Financial: 10.752, Safety: 2.24, Privacy: 2.24
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: A domain name server translates a domain name (such as www.example.com) into an IP address that Internet hosts use to contact Internet resources. An adversary modifies a public DNS cache to cause cert...

- Command Delimiters
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.8
  Risk Scores: Financial: 2.24, Safety: 2.24, Privacy: 10.752
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: An attack of this type exploits a programs' vulnerabilities that allows an attacker's commands to be concatenated onto a legitimate command with the intent of targeting other resources such as the fil...

- Malicious Automated Software Update via Redirection
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.8
  Risk Scores: Financial: 2.24, Safety: 2.24, Privacy: 10.752
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: An attacker exploits two layers of weaknesses in server or client software for automated update mechanisms to undermine the integrity of the target code-base. The first weakness involves a failure to ...

- PHP Remote File Inclusion
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.8
  Risk Scores: Financial: 2.24, Safety: 2.24, Privacy: 10.752
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: In this pattern the adversary is able to load and execute arbitrary code remotely available from the application. This is usually accomplished through an insecurely configured PHP runtime environment ...

- XSS Using Alternate Syntax
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.8
  Risk Scores: Financial: 2.24, Safety: 2.24, Privacy: 10.752
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20

Description: An adversary uses alternate forms of keywords or commands that result in the same action as the primary form but which may not be caught by filters. For example, many keywords are processed in a case ...

- Serialized Data External Linking
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.8
  Risk Scores: Financial: 2.24, Safety: 2.24, Privacy: 10.752
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: An adversary creates a serialized data file (e.g. XML, YAML, etc...) that contains an external data reference. Because serialized data parsers may not validate documents with external references, ther...

- Leveraging Race Conditions
  Impact Scores: Financial: 4.8, Safety: 1, Privacy: 1
  Risk Scores: Financial: 10.752, Safety: 2.24, Privacy: 2.24
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: The adversary targets a race condition occurring when multiple processes access and manipulate the same resource concurrently, and the outcome of the execution depends on the particular order in which...

- Leveraging Time-of-Check and Time-of-Use (TOCTOU) Race Conditions
  Impact Scores: Financial: 4.8, Safety: 1, Privacy: 1
  Risk Scores: Financial: 10.752, Safety: 2.24, Privacy: 2.24
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: This attack targets a race condition occurring between the time of check (state) for a resource and the time of use of a resource. A typical example is file access. The adversary can leverage a file a...

- Using Meta-characters in E-mail Headers to Inject Malicious Payloads
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.8
  Risk Scores: Financial: 2.24, Safety: 2.24, Privacy: 10.752
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: This type of attack involves an attacker leveraging meta-characters in email headers to inject improper behavior into email programs. Email software has become increasingly sophisticated and feature-r...

- Buffer Overflow via Symbolic Links
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.8
  Risk Scores: Financial: 2.24, Safety: 2.24, Privacy: 10.752
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: This type of attack leverages the use of symbolic links to cause buffer overflows. An adversary can try to create or manipulate a symbolic link file such that its contents result in out of bounds data...

- Passing Local Filenames to Functions That Expect a URL
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.8
  Risk Scores: Financial: 2.24, Safety: 2.24, Privacy: 10.752
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: This attack relies on client side code to access local files and resources instead of URLs. When the client browser is expecting a URL string, but instead receives a request for a local file, that exe...

- Session Credential Falsification through Prediction
  Impact Scores: Financial: 4.8, Safety: 1, Privacy: 1
  Risk Scores: Financial: 10.752, Safety: 2.24, Privacy: 2.24
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: This attack targets predictable session ID in order to gain privileges. The attacker can predict the session ID used during a transaction to perform spoofing and session hijacking....

- Using Slashes and URL Encoding Combined to Bypass Validation Logic

Impact Scores: Financial: 4.8, Safety: 1, Privacy: 1
Risk Scores: Financial: 10.752, Safety: 2.24, Privacy: 2.24
Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
Description: This attack targets the encoding of the URL combined with the encoding of the slash characters. An attacker can take advantage of the multiple ways of encoding a URL and abuse the interpretation of th...

- Voice Phishing
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.8
  Risk Scores: Financial: 2.24, Safety: 2.24, Privacy: 10.752
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: An adversary targets users with a phishing attack for the purpose of soliciting account passwords or sensitive information from the user. Voice Phishing is a variation of the Phishing social engineeri...

- Malicious Automated Software Update via Spoofing
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.8
  Risk Scores: Financial: 2.24, Safety: 2.24, Privacy: 10.752
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: An attackers uses identify or content spoofing to trick a client into performing an automated software update from a malicious source. A malicious automated software update that leverages spoofing can...

- Blind SQL Injection
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.8
  Risk Scores: Financial: 2.24, Safety: 2.24, Privacy: 10.752
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: Blind SQL Injection results from an insufficient mitigation for SQL Injection. Although suppressing database error messages are considered best practice, the suppression alone is not sufficient to pre...

- URL Encoding
  Impact Scores: Financial: 4.8, Safety: 1, Privacy: 1
  Risk Scores: Financial: 10.752, Safety: 2.24, Privacy: 2.24
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: This attack targets the encoding of the URL. An adversary can take advantage of the multiple way of encoding an URL and abuse the interpretation of the URL....

- User-Controlled Filename
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.8
  Risk Scores: Financial: 2.24, Safety: 2.24, Privacy: 10.752
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: An attack of this type involves an adversary inserting malicious characters (such as a XSS redirection) into a filename, directly or indirectly that is then used by the target software to generate HTM...

- Using Escaped Slashes in Alternate Encoding
  Impact Scores: Financial: 4.8, Safety: 1, Privacy: 1
  Risk Scores: Financial: 10.752, Safety: 2.24, Privacy: 2.24
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: This attack targets the use of the backslash in alternate encoding. An adversary can provide a backslash as a leading character and causes a parser to believe that the next character is special. This ...

- Buffer Overflow in an API Call
  Impact Scores: Financial: 4.8, Safety: 1, Privacy: 1
  Risk Scores: Financial: 10.752, Safety: 2.24, Privacy: 2.24
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: This attack targets libraries or shared code modules which are vulnerable to buffer overflow attacks. An

adversary who has knowledge of known vulnerable libraries or shared code can easily target soft...

- Using UTF-8 Encoding to Bypass Validation Logic
  Impact Scores: Financial: 1, Safety: 4.8, Privacy: 1
  Risk Scores: Financial: 2.24, Safety: 10.752, Privacy: 2.24
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: This attack is a specific variation on leveraging alternate encodings to bypass validation logic. This attack leverages the possibility to encode potentially harmful input in UTF-8 and submit it to ap...

- XPath Injection
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.8
  Risk Scores: Financial: 2.24, Safety: 2.24, Privacy: 10.752
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: An attacker can craft special user-controllable input consisting of XPath expressions to inject the XML database and bypass authentication or glean information that they normally would not be able to....

- OS Command Injection
  Impact Scores: Financial: 4.8, Safety: 1, Privacy: 1
  Risk Scores: Financial: 10.752, Safety: 2.24, Privacy: 2.24
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: In this type of an attack, an adversary injects operating system commands into existing application functions. An application that uses untrusted input to build command strings is vulnerable. An adver...

- Buffer Overflow in Local Command-Line Utilities
  Impact Scores: Financial: 4.8, Safety: 1, Privacy: 1
  Risk Scores: Financial: 10.752, Safety: 2.24, Privacy: 2.24
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: This attack targets command-line utilities available in a number of shells. An adversary can leverage a vulnerability found in a command-line utility to escalate privilege to root....

- Reflection Attack in Authentication Protocol
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.8
  Risk Scores: Financial: 2.24, Safety: 2.24, Privacy: 10.752
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: An adversary can abuse an authentication protocol susceptible to reflection attack in order to defeat it. Doing so allows the adversary illegitimate access to the target system, without possessing the...

- Forced Integer Overflow
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.8
  Risk Scores: Financial: 2.24, Safety: 2.24, Privacy: 10.752
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: This attack forces an integer variable to go out of range. The integer variable is often used as an offset such as size of memory allocation or similarly. The attacker would typically control the valu...

- WSDL Scanning
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.8
  Risk Scores: Financial: 2.24, Safety: 2.24, Privacy: 10.752
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: This attack targets the WSDL interface made available by a web service. The attacker may scan the WSDL interface to reveal sensitive information about invocation patterns, underlying technology implem...

- Root/Jailbreak Detection Evasion via Debugging
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5

  Risk Scores: Financial: 1.6800000000000002, Safety: 1.6800000000000002, Privacy: 8.4
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: An adversary inserts a debugger into the program entry point of a mobile application to modify the application binary, with the goal of evading Root/Jailbreak detection. Mobile device users often Root...

- CAN Injection
  Impact Scores: Financial: 3.5999999999999996, Safety: 4.8, Privacy: 2.4
  Risk Scores: Financial: 6.048, Safety: 8.064, Privacy: 4.032
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: Manipulation of CAN bus messages leading to vehicle malfunction...

- HTTP Request Splitting
  Impact Scores: Financial: 4.8, Safety: 1, Privacy: 1
  Risk Scores: Financial: 8.064, Safety: 1.6800000000000002, Privacy: 1.6800000000000002
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: An adversary abuses the flexibility and discrepancies in the parsing and interpretation of HTTP Request messages by different intermediary HTTP agents (e.g., load balancer, reverse proxy, web caching ...

- Flooding
  Impact Scores: Financial: 1, Safety: 1.2, Privacy: 3.5999999999999996
  Risk Scores: Financial: 2.24, Safety: 2.688, Privacy: 8.064
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: An adversary consumes the resources of a target by rapidly engaging in a large number of interactions with the target. This type of attack generally exposes a weakness in rate limiting or flow. When s...

- Directory Indexing
  Impact Scores: Financial: 1, Safety: 1, Privacy: 3.5999999999999996
  Risk Scores: Financial: 2.24, Safety: 2.24, Privacy: 8.064
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: An adversary crafts a request to a target that results in the target listing/indexing the content of a directory as output. One common method of triggering directory contents as output is to construct...

- Flash Parameter Injection
  Impact Scores: Financial: 1, Safety: 1, Privacy: 3.5999999999999996
  Risk Scores: Financial: 2.24, Safety: 2.24, Privacy: 8.064
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: An adversary takes advantage of improper data validation to inject malicious global parameters into a Flash file embedded within an HTML document. Flash files can leverage user-submitted data to confi...

- Exploiting Incorrectly Configured Access Control Security Levels
  Impact Scores: Financial: 1, Safety: 1, Privacy: 3.5999999999999996
  Risk Scores: Financial: 2.24, Safety: 2.24, Privacy: 8.064
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: An attacker exploits a weakness in the configuration of access controls and is able to bypass the intended protection that these measures guard against and thereby obtain unauthorized access to the sy...

- Exponential Data Expansion
  Impact Scores: Financial: 1, Safety: 1, Privacy: 3.5999999999999996
  Risk Scores: Financial: 2.24, Safety: 2.24, Privacy: 8.064
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: An adversary submits data to a target application which contains nested exponential data expansion to produce excessively large output. Many data format languages allow the definition of macro-like st...

- Inducing Account Lockout
  Impact Scores: Financial: 1, Safety: 1, Privacy: 3.5999999999999996
  Risk Scores: Financial: 2.24, Safety: 2.24, Privacy: 8.064
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: An attacker leverages the security functionality of the system aimed at thwarting potential attacks to launch a denial of service attack against a legitimate system user. Many systems, for instance, i...

- XML Routing Detour Attacks
  Impact Scores: Financial: 1, Safety: 1, Privacy: 3.5999999999999996
  Risk Scores: Financial: 2.24, Safety: 2.24, Privacy: 8.064
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: An attacker subverts an intermediate system used to process XML content and forces the intermediate to modify and/or re-route the processing of the content. XML Routing Detour Attacks are Adversary in...

- Serialized Data with Nested Payloads
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.8
  Risk Scores: Financial: 1.6800000000000002, Safety: 1.6800000000000002, Privacy: 8.064
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: Applications often need to transform data in and out of a data format (e.g., XML and YAML) by using a parser. It may be possible for an adversary to inject data that may have an adverse effect on the ...

- Command Injection
  Impact Scores: Financial: 4.8, Safety: 1, Privacy: 1
  Risk Scores: Financial: 8.064, Safety: 1.6800000000000002, Privacy: 1.6800000000000002
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: An adversary looking to execute a command of their choosing, injects new items into an existing command thus modifying interpretation away from what was intended. Commands in this context are often st...

- Leveraging Race Conditions via Symbolic Links
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.8
  Risk Scores: Financial: 1.6800000000000002, Safety: 1.6800000000000002, Privacy: 8.064
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: This attack leverages the use of symbolic links (Symlinks) in order to write to sensitive files. An attacker can create a Symlink link to a target file not otherwise accessible to them. When the privi...

- HTTP Response Smuggling
  Impact Scores: Financial: 4.8, Safety: 1, Privacy: 1
  Risk Scores: Financial: 8.064, Safety: 1.6800000000000002, Privacy: 1.6800000000000002
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: An adversary manipulates and injects malicious content in the form of secret unauthorized HTTP responses, into a single HTTP response from a vulnerable or compromised back-end HTTP agent (e.g., server...

- SOAP Manipulation
  Impact Scores: Financial: 4.8, Safety: 1, Privacy: 1
  Risk Scores: Financial: 8.064, Safety: 1.6800000000000002, Privacy: 1.6800000000000002
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: Simple Object Access Protocol (SOAP) is used as a communication protocol between a client and server to invoke web services on the server. It is an XML-based protocol, and therefore suffers from many ...

- Fuzzing
  Impact Scores: Financial: 1, Safety: 1, Privacy: 3.5999999999999996
  Risk Scores: Financial: 2.24, Safety: 2.24, Privacy: 8.064
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20

Description: In this attack pattern, the adversary leverages fuzzing to try to identify weaknesses in the system. Fuzzing is a software security and functionality testing method that feeds randomly constructed inp...

- HTTP Request Smuggling
  Impact Scores: Financial: 4.8, Safety: 1, Privacy: 1
  Risk Scores: Financial: 8.064, Safety: 1.6800000000000002, Privacy: 1.6800000000000002
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: An adversary abuses the flexibility and discrepancies in the parsing and interpretation of HTTP Request messages using various HTTP headers, request-line and body parameters as well as message sizes (...

- HTTP Response Splitting
  Impact Scores: Financial: 4.8, Safety: 1, Privacy: 1
  Risk Scores: Financial: 8.064, Safety: 1.6800000000000002, Privacy: 1.6800000000000002
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: An adversary manipulates and injects malicious content, in the form of secret unauthorized HTTP responses, into a single HTTP response from a vulnerable or compromised back-end HTTP agent (e.g., web s...

- Manipulating Opaque Client-based Data Tokens
  Impact Scores: Financial: 1, Safety: 1, Privacy: 3.5999999999999996
  Risk Scores: Financial: 2.24, Safety: 2.24, Privacy: 8.064
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: In circumstances where an application holds important data client-side in tokens (cookies, URLs, data files, and so forth) that data can be manipulated. If client or server-side application components...

- Using Alternative IP Address Encodings
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.8
  Risk Scores: Financial: 1.6800000000000002, Safety: 1.6800000000000002, Privacy: 8.064
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: This attack relies on the adversary using unexpected formats for representing IP addresses. Networked applications may expect network location information in a specific format, such as fully qualified...

- Exploiting Multiple Input Interpretation Layers
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.8
  Risk Scores: Financial: 1.6800000000000002, Safety: 1.6800000000000002, Privacy: 8.064
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: An attacker supplies the target software with input data that contains sequences of special characters designed to bypass input validation logic. This exploit relies on the target making multiples pas...

- Development Alteration
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.8
  Risk Scores: Financial: 1.6800000000000002, Safety: 1.6800000000000002, Privacy: 8.064
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: An adversary modifies a technology, product, or component during its development to acheive a negative impact once the system is deployed. The goal of the adversary is to modify the system in such a w...

- Malicious Logic Insertion into Product Software via Configuration Management Manipulation
  Impact Scores: Financial: 4.8, Safety: 1, Privacy: 1
  Risk Scores: Financial: 8.064, Safety: 1.6800000000000002, Privacy: 1.6800000000000002
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: An adversary exploits a configuration management system so that malicious logic is inserted into a software products build, update or deployed environment. If an adversary can control the elements inc...

- Design Alteration

Impact Scores: Financial: 1, Safety: 1, Privacy: 4.8
Risk Scores: Financial: 1.6800000000000002, Safety: 1.6800000000000002, Privacy: 8.064
Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
Description: An adversary modifies the design of a technology, product, or component to acheive a negative impact once the system is deployed. In this type of attack, the goal of the adversary is to modify the des...

- Contradictory Destinations in Traffic Routing Schemes
  Impact Scores: Financial: 4.8, Safety: 1, Privacy: 1
  Risk Scores: Financial: 8.064, Safety: 1.6800000000000002, Privacy: 1.6800000000000002
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: Adversaries can provide contradictory destinations when sending messages. Traffic is routed in networks using the domain names in various headers available at different levels of the OSI model. In a C...

- Object Injection
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.8
  Risk Scores: Financial: 1.6800000000000002, Safety: 1.6800000000000002, Privacy: 8.064
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: An adversary attempts to exploit an application by injecting additional, malicious content during its processing of serialized objects. Developers leverage serialization in order to convert data or st...

- Bluetooth Impersonation AttackS (BIAS)
  Impact Scores: Financial: 4.8, Safety: 1, Privacy: 1
  Risk Scores: Financial: 8.064, Safety: 1.6800000000000002, Privacy: 1.6800000000000002
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: An adversary disguises the MAC address of their Bluetooth enabled device to one for which there exists an active and trusted connection and authenticates successfully. The adversary can then perform m...

- Alteration of a Software Update
  Impact Scores: Financial: 4.8, Safety: 1, Privacy: 1
  Risk Scores: Financial: 8.064, Safety: 1.6800000000000002, Privacy: 1.6800000000000002
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: An adversary with access to an organization’s software update infrastructure inserts malware into the content of an outgoing update to fielded systems where a wide range of malicious effects are possi...

- Eavesdropping on a Monitor
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.8
  Risk Scores: Financial: 1.6800000000000002, Safety: 1.6800000000000002, Privacy: 8.064
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: An Adversary can eavesdrop on the content of an external monitor through the air without modifying any cable or installing software, just capturing this signal emitted by the cable or video port, with...

- Browser in the Middle (BiTM)
  Impact Scores: Financial: 4.8, Safety: 1, Privacy: 1
  Risk Scores: Financial: 8.064, Safety: 1.6800000000000002, Privacy: 1.6800000000000002
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: An adversary exploits the inherent functionalities of a web browser, in order to establish an unnoticed remote desktop connection in the victim's browser to the adversary's system. The adversary must ...

- Manipulating State
  Impact Scores: Financial: 1.2, Safety: 1, Privacy: 4.8
  Risk Scores: Financial: 2.016, Safety: 1.6800000000000002, Privacy: 8.064
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: The adversary modifies state information maintained by the target software or causes a state transition in

hardware. If successful, the target will use this tainted state and execute in an unintended ...

- Interface Manipulation
  Impact Scores: Financial: 3.5999999999999996, Safety: 1, Privacy: 1
  Risk Scores: Financial: 6.048, Safety: 1.6800000000000002, Privacy: 1.6800000000000002
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: An adversary manipulates the use or processing of an interface (e.g. Application Programming Interface (API) or System-on-Chip (SoC)) resulting in an adverse impact upon the security of the system imp...

- Parameter Injection
  Impact Scores: Financial: 1, Safety: 1, Privacy: 3.5999999999999996
  Risk Scores: Financial: 1.6800000000000002, Safety: 1.6800000000000002, Privacy: 6.048
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: An adversary manipulates the content of request parameters for the purpose of undermining the security of the target. Some parameter encodings use text characters as separators. For example, parameter...

- Content Spoofing
  Impact Scores: Financial: 3.5999999999999996, Safety: 1, Privacy: 3.5999999999999996
  Risk Scores: Financial: 6.048, Safety: 1.6800000000000002, Privacy: 6.048
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: An adversary modifies content to make it contain something other than what the original content producer intended while keeping the apparent source of the content unchanged. The term content spoofing ...

- Resource Location Spoofing
  Impact Scores: Financial: 1, Safety: 1, Privacy: 3.5999999999999996
  Risk Scores: Financial: 1.6800000000000002, Safety: 1.6800000000000002, Privacy: 6.048
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: An adversary deceives an application or user and convinces them to request a resource from an unintended location. By spoofing the location, the adversary can cause an alternate resource to be used, o...

- Cross-Site Flashing
  Impact Scores: Financial: 3.5999999999999996, Safety: 1, Privacy: 1
  Risk Scores: Financial: 6.048, Safety: 1.6800000000000002, Privacy: 1.6800000000000002
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: An attacker is able to trick the victim into executing a Flash document that passes commands or calls to a Flash player browser plugin, allowing the attacker to exploit native Flash functionality in t...

- Modification of Registry Run Keys
  Impact Scores: Financial: 1, Safety: 1, Privacy: 3.5999999999999996
  Risk Scores: Financial: 1.6800000000000002, Safety: 1.6800000000000002, Privacy: 6.048
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: An adversary adds a new entry to the run keys in the Windows registry so that an application of their choosing is executed when a user logs in. In this way, the adversary can get their executable to o...

- Using Leading 'Ghost' Character Sequences to Bypass Input Filters
  Impact Scores: Financial: 1, Safety: 1, Privacy: 3.5999999999999996
  Risk Scores: Financial: 1.6800000000000002, Safety: 1.6800000000000002, Privacy: 6.048
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: Some APIs will strip certain leading characters from a string of parameters. An adversary can intentionally introduce leading ghost characters (extra characters that don't affect the validity of the r...

- Manipulate Human Behavior
  Impact Scores: Financial: 1, Safety: 1, Privacy: 3.5999999999999996

```
  Risk Scores: Financial: 1.6800000000000002, Safety: 1.6800000000000002, Privacy: 6.048
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: An adversary exploits inherent human psychological predisposition to influence a targeted individual or group to solicit information or manipulate the target into performing an action that serves the ...

- Disable Security Software
  Impact Scores: Financial: 3.5999999999999996, Safety: 1, Privacy: 1
  Risk Scores: Financial: 6.048, Safety: 1.6800000000000002, Privacy: 1.6800000000000002
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: An adversary exploits a weakness in access control to disable security tools so that detection does not occur. This can take the form of killing processes, deleting registry keys so that tools do not ...

- Collect Data from Registries
  Impact Scores: Financial: 1, Safety: 1, Privacy: 3.5999999999999996
  Risk Scores: Financial: 1.6800000000000002, Safety: 1.6800000000000002, Privacy: 6.048
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: An adversary exploits a weakness in authorization to gather system-specific data and sensitive information within a registry (e.g., Windows Registry, Mac plist). These contain information about the sy...

- Collect Data from Screen Capture
  Impact Scores: Financial: 1, Safety: 1, Privacy: 3.5999999999999996
  Risk Scores: Financial: 1.6800000000000002, Safety: 1.6800000000000002, Privacy: 6.048
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: An adversary gathers sensitive information by exploiting the system's screen capture functionality. Through screenshots, the adversary aims to see what happens on the screen over the course of an oper...

- Retrieve Data from Decommissioned Devices
  Impact Scores: Financial: 1, Safety: 1.2, Privacy: 3.5999999999999996
  Risk Scores: Financial: 1.6800000000000002, Safety: 2.016, Privacy: 6.048
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: An adversary obtains decommissioned, recycled, or discarded systems and devices that can include an organization’s intellectual property, employee data, and other types of controlled information. Syst...

- Escaping a Sandbox by Calling Code in Another Language
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5
  Risk Scores: Financial: 1.12, Safety: 1.12, Privacy: 5.6000000000000005
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: The attacker may submit malicious code of another language to obtain access to privileges that were not intentionally exposed by the sandbox, thus escaping the sandbox. For instance, Java code cannot ...

- Hijacking a Privileged Thread of Execution
  Impact Scores: Financial: 5, Safety: 1, Privacy: 1
  Risk Scores: Financial: 5.6000000000000005, Safety: 1.12, Privacy: 1.12
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: An adversary hijacks a privileged thread of execution by injecting malicious code into a running process. By using a privleged thread to do their bidding, adversaries can evade process-based detection...

- Subvert Code-signing Facilities
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5
  Risk Scores: Financial: 1.12, Safety: 1.12, Privacy: 5.6000000000000005
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: Many languages use code signing facilities to vouch for code's identity and to thus tie code to its assigned privileges within an environment. Subverting this mechanism can be instrumental in an attac...
```

```
- Load Value Injection
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5
  Risk Scores: Financial: 1.12, Safety: 1.12, Privacy: 5.6000000000000005
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: An adversary exploits a hardware design flaw in a CPU implementation of transient instruction execution in which a faulting or assisted load instruction transiently forwards adversary-controlled data ...

- Web Application Fingerprinting
  Impact Scores: Financial: 1, Safety: 1, Privacy: 2.4
  Risk Scores: Financial: 2.24, Safety: 2.24, Privacy: 5.376
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: An attacker sends a series of probes to a web application in order to elicit version-dependent and type-dependent behavior that assists in identifying the target. An attacker could learn information s...

- Fuzzing for application mapping
  Impact Scores: Financial: 1, Safety: 2.4, Privacy: 1
  Risk Scores: Financial: 2.24, Safety: 5.376, Privacy: 2.24
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: An attacker sends random, malformed, or otherwise unexpected messages to a target application and observes the application's log or error messages returned. The attacker does not initially know how a ...

- Forced Deadlock
  Impact Scores: Financial: 4.8, Safety: 1, Privacy: 1
  Risk Scores: Financial: 5.376, Safety: 1.12, Privacy: 1.12
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: The adversary triggers and exploits a deadlock condition in the target software to cause a denial of service. A deadlock can occur when two or more competing actions are waiting for each other to fini...

- Schema Poisoning
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.8
  Risk Scores: Financial: 1.12, Safety: 1.12, Privacy: 5.376
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: An adversary corrupts or modifies the content of a schema for the purpose of undermining the security of the target. Schemas provide the structure and content definitions for resources used by an appl...

- USB Memory Attacks
  Impact Scores: Financial: 2.4, Safety: 1, Privacy: 4.8
  Risk Scores: Financial: 2.688, Safety: 1.12, Privacy: 5.376
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: An adversary loads malicious code onto a USB memory stick in order to infect any system which the device is plugged in to. USB drives present a significant security risk for business and government ag...

- Signature Spoofing by Misrepresentation
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.8
  Risk Scores: Financial: 1.12, Safety: 1.12, Privacy: 5.376
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: An attacker exploits a weakness in the parsing or display code of the recipient software to generate a data blob containing a supposedly valid signature, but the signer's identity is falsely represent...

- Hardware Component Substitution During Baselining
  Impact Scores: Financial: 4.8, Safety: 1, Privacy: 1
  Risk Scores: Financial: 5.376, Safety: 1.12, Privacy: 1.12
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
```

Description: An adversary with access to system components during allocated baseline development can substitute a maliciously altered hardware component for a baseline component during the product development and ...

- Malicious Hardware Update
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.8
  Risk Scores: Financial: 1.12, Safety: 1.12, Privacy: 5.376
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: An adversary introduces malicious hardware during an update or replacement procedure, allowing for additional compromise or site disruption at the victim location. After deployment, it is not uncommon...

- Open-Source Library Manipulation
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.8
  Risk Scores: Financial: 1.12, Safety: 1.12, Privacy: 5.376
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: Adversaries implant malicious code in open source software (OSS) libraries to have it widely distributed, as OSS is commonly downloaded by developers and other users to incorporate into software devel...

- ASIC With Malicious Functionality
  Impact Scores: Financial: 4.8, Safety: 1, Privacy: 1
  Risk Scores: Financial: 5.376, Safety: 1.12, Privacy: 1.12
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: An attacker with access to the development environment process of an application-specific integrated circuit (ASIC) for a victim system being developed or maintained after initial deployment can inser...

- Hardware Fault Injection
  Impact Scores: Financial: 1, Safety: 4.8, Privacy: 4.8
  Risk Scores: Financial: 1.12, Safety: 5.376, Privacy: 5.376
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: The adversary uses disruptive signals or events, or alters the physical environment a device operates in, to cause faulty behavior in electronic devices. This can include electromagnetic pulses, laser...

- Carry-Off GPS Attack
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.8
  Risk Scores: Financial: 1.12, Safety: 1.12, Privacy: 5.376
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: A common form of a GPS spoofing attack, commonly termed a carry-off attack begins with an adversary broadcasting signals synchronized with the genuine signals observed by the target receiver. The powe...

- DLL Side-Loading
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.8
  Risk Scores: Financial: 1.12, Safety: 1.12, Privacy: 5.376
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: An adversary places a malicious version of a Dynamic-Link Library (DLL) in the Windows Side-by-Side (WinSxS) directory to trick the operating system into loading this malicious DLL instead of a legiti...

- Use of Captured Tickets (Pass The Ticket)
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.8
  Risk Scores: Financial: 1.12, Safety: 1.12, Privacy: 5.376
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: An adversary uses stolen Kerberos tickets to access systems/resources that leverage the Kerberos authentication protocol. The Kerberos authentication protocol centers around a ticketing system which i...

- Sniff Application Code

```
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.8
  Risk Scores: Financial: 1.12, Safety: 1.12, Privacy: 5.376
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
```

Description: An adversary passively sniffs network communications and captures application code bound for an authorized client. Once obtained, they can use it as-is, or through reverse-engineering glean sensitive ...

```
- Key Negotiation of Bluetooth Attack (KNOB)
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.8
  Risk Scores: Financial: 1.12, Safety: 1.12, Privacy: 5.376
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
```

Description: An adversary can exploit a flaw in Bluetooth key negotiation allowing them to decrypt information sent between two devices communicating via Bluetooth. The adversary uses an Adversary in the Middle se...

```
- Malicious Code Implanted During Chip Programming
  Impact Scores: Financial: 4.8, Safety: 1, Privacy: 1
  Risk Scores: Financial: 5.376, Safety: 1.12, Privacy: 1.12
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
```

Description: During the programming step of chip manufacture, an adversary with access and necessary technical skills maliciously alters a chip’s intended program logic to produce an effect intended by the adversa...

```
- AJAX Footprinting
  Impact Scores: Financial: 1, Safety: 1, Privacy: 2.4
  Risk Scores: Financial: 2.24, Safety: 2.24, Privacy: 5.376
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
```

Description: This attack utilizes the frequent client-server roundtrips in Ajax conversation to scan a system. While Ajax does not open up new vulnerabilities per se, it does optimize them from an attacker point o...

```
- Interception
  Impact Scores: Financial: 1, Safety: 1, Privacy: 3.5999999999999996
  Risk Scores: Financial: 1.12, Safety: 1.12, Privacy: 4.032
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
```

Description: An adversary monitors data streams to or from the target for information gathering purposes. This attack may be undertaken to solely gather sensitive information or to support a further attack against...

```
- XML Ping of the Death
  Impact Scores: Financial: 1, Safety: 3.5999999999999996, Privacy: 1
  Risk Scores: Financial: 1.12, Safety: 4.032, Privacy: 1.12
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
```

Description: An attacker initiates a resource depletion attack where a large number of small XML messages are delivered at a sufficiently rapid rate to cause a denial of service or crash of the target. Transaction...

```
- Active OS Fingerprinting
  Impact Scores: Financial: 1, Safety: 1, Privacy: 2.4
  Risk Scores: Financial: 1.6800000000000002, Safety: 1.6800000000000002, Privacy: 4.032
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
```

Description: An adversary engages in activity to detect the operating system or firmware version of a remote target by interrogating a device, server, or platform with a probe designed to solicit behavior that wil...

```
- TCP Timestamp Probe
  Impact Scores: Financial: 2.4, Safety: 1, Privacy: 1
  Risk Scores: Financial: 4.032, Safety: 1.6800000000000002, Privacy: 1.6800000000000002
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
```

Description: This OS fingerprinting probe examines the remote server's implementation of TCP timestamps. Not all operating systems implement timestamps within the TCP header, but when timestamps are used then this...

- TCP Sequence Number Probe
  Impact Scores: Financial: 2.4, Safety: 1, Privacy: 1
  Risk Scores: Financial: 4.032, Safety: 1.6800000000000002, Privacy: 1.6800000000000002
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: This OS fingerprinting probe tests the target system's assignment of TCP sequence numbers. One common way to test TCP Sequence Number generation is to send a probe packet to an open port on the target...

- TCP (ISN) Greatest Common Divisor Probe
  Impact Scores: Financial: 1, Safety: 1, Privacy: 2.4
  Risk Scores: Financial: 1.6800000000000002, Safety: 1.6800000000000002, Privacy: 4.032
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: This OS fingerprinting probe sends a number of TCP SYN packets to an open port of a remote machine. The Initial Sequence Number (ISN) in each of the SYN/ACK response packets is analyzed to determine t...

- TCP (ISN) Counter Rate Probe
  Impact Scores: Financial: 1, Safety: 1, Privacy: 2.4
  Risk Scores: Financial: 1.6800000000000002, Safety: 1.6800000000000002, Privacy: 4.032
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: This OS detection probe measures the average rate of initial sequence number increments during a period of time. Sequence numbers are incremented using a time-based algorithm and are susceptible to a ...

- TCP (ISN) Sequence Predictability Probe
  Impact Scores: Financial: 1, Safety: 1, Privacy: 2.4
  Risk Scores: Financial: 1.6800000000000002, Safety: 1.6800000000000002, Privacy: 4.032
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: This type of operating system probe attempts to determine an estimate for how predictable the sequence number generation algorithm is for a remote host. Statistical techniques, such as standard deviat...

- TCP Initial Window Size Probe
  Impact Scores: Financial: 2.4, Safety: 1, Privacy: 1
  Risk Scores: Financial: 4.032, Safety: 1.6800000000000002, Privacy: 1.6800000000000002
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: This OS fingerprinting probe checks the initial TCP Window size. TCP stacks limit the range of sequence numbers allowable within a session to maintain the connected state within TCP protocol logic. Th...

- TCP Options Probe
  Impact Scores: Financial: 2.4, Safety: 1, Privacy: 1
  Risk Scores: Financial: 4.032, Safety: 1.6800000000000002, Privacy: 1.6800000000000002
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: This OS fingerprinting probe analyzes the type and order of any TCP header options present within a response segment. Most operating systems use unique ordering and different option sets when options ...

- Pretexting
  Impact Scores: Financial: 1, Safety: 1, Privacy: 2.4
  Risk Scores: Financial: 1.6800000000000002, Safety: 1.6800000000000002, Privacy: 4.032
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: An adversary engages in pretexting behavior to solicit information from target persons, or manipulate the target into performing some action that serves the adversary's interests. During a pretexting ...

- Incomplete Data Deletion in a Multi-Tenant Environment
  Impact Scores: Financial: 1, Safety: 1, Privacy: 3.5999999999999996

Risk Scores: Financial: 1.12, Safety: 1.12, Privacy: 4.032
Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
Description: An adversary obtains unauthorized information due to insecure or incomplete data deletion in a multi-tenant environment. If a cloud provider fails to completely delete storage and data from former clo...

- Adding a Space to a File Extension
  Impact Scores: Financial: 1, Safety: 1, Privacy: 3.5999999999999996
  Risk Scores: Financial: 1.12, Safety: 1.12, Privacy: 4.032
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: An adversary adds a space character to the end of a file extension and takes advantage of an application that does not properly neutralize trailing special elements in file names. This extra space, wh...

- Reverse Engineering
  Impact Scores: Financial: 2.4, Safety: 1, Privacy: 1
  Risk Scores: Financial: 2.688, Safety: 1.12, Privacy: 1.12
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: An adversary discovers the structure, function, and composition of an object, resource, or system by using a variety of analysis techniques to effectively determine how the analyzed entity was constru...

- Fingerprinting
  Impact Scores: Financial: 1, Safety: 1, Privacy: 1.2
  Risk Scores: Financial: 2.24, Safety: 2.24, Privacy: 2.688
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: An adversary compares output from a target system to known indicators that uniquely identify specific details about the target. Most commonly, fingerprinting is done to determine operating system and ...

- Target Influence via Framing
  Impact Scores: Financial: 1, Safety: 1.2, Privacy: 2.4
  Risk Scores: Financial: 1.12, Safety: 1.344, Privacy: 2.688
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: An adversary uses framing techniques to contextualize a conversation so that the target is more likely to be influenced by the adversary's point of view. Framing is information and experiences in life...

- Influence via Psychological Principles
  Impact Scores: Financial: 2.4, Safety: 1, Privacy: 1
  Risk Scores: Financial: 2.688, Safety: 1.12, Privacy: 1.12
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: The adversary shapes the target's actions or behavior by focusing on the ways human interact and learn, leveraging such elements as cognitive and social psychology. In a variety of ways, a target can ...

- Process Footprinting
  Impact Scores: Financial: 1, Safety: 1, Privacy: 2.4
  Risk Scores: Financial: 1.12, Safety: 1.12, Privacy: 2.688
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: An adversary exploits functionality meant to identify information about the currently running processes on the target system to an authorized user. By knowing what processes are running on the target ...

- Services Footprinting
  Impact Scores: Financial: 1, Safety: 1, Privacy: 2.4
  Risk Scores: Financial: 1.12, Safety: 1.12, Privacy: 2.688
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: An adversary exploits functionality meant to identify information about the services on the target system to an authorized user. By knowing what services are registered on the target system, the adver...

- Account Footprinting
  Impact Scores: Financial: 1, Safety: 1, Privacy: 2.4
  Risk Scores: Financial: 1.12, Safety: 1.12, Privacy: 2.688
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: An adversary exploits functionality meant to identify information about the domain accounts and their permissions on the target system to an authorized user. By knowing what accounts are registered on...

- Group Permission Footprinting
  Impact Scores: Financial: 1, Safety: 1, Privacy: 2.4
  Risk Scores: Financial: 1.12, Safety: 1.12, Privacy: 2.688
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: An adversary exploits functionality meant to identify information about user groups and their permissions on the target system to an authorized user. By knowing what users/permissions are registered o...

- Owner Footprinting
  Impact Scores: Financial: 1, Safety: 1, Privacy: 2.4
  Risk Scores: Financial: 1.12, Safety: 1.12, Privacy: 2.688
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: An adversary exploits functionality meant to identify information about the primary users on the target system to an authorized user. They may do this, for example, by reviewing logins or file modific...

- System Footprinting
  Impact Scores: Financial: 1, Safety: 1, Privacy: 2.4
  Risk Scores: Financial: 1.12, Safety: 1.12, Privacy: 2.688
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: An adversary engages in active probing and exploration activities to determine security information about a remote target system. Often times adversaries will rely on remote applications that can be p...

- Collect Data from Clipboard
  Impact Scores: Financial: 1, Safety: 1, Privacy: 2.4
  Risk Scores: Financial: 1.12, Safety: 1.12, Privacy: 2.688
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: The adversary exploits an application that allows for the copying of sensitive data or information by collecting information copied to the clipboard. Data copied to the clipboard can be accessed by ot...

Component: Brake Actuator

Type: Actuator
Safety Level: ASIL D
Interfaces: CAN
Access Points:
Data Types: Control Commands
Location: Internal
Trust Zone: Critical
Connected To: ECU003

Identified Threats:

- Accessing Functionality Not Properly Constrained by ACLs
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5
  Risk Scores: Financial: 2.24, Safety: 2.24, Privacy: 11.200000000000001

Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
Description: In applications, particularly web applications, access to functionality is mitigated by an authorization framework. This framework maps Access Control Lists (ACLs) to elements of the application's fun...

- Buffer Overflow via Environment Variables
  Impact Scores: Financial: 5, Safety: 1, Privacy: 1
  Risk Scores: Financial: 11.200000000000001, Safety: 2.24, Privacy: 2.24
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: This attack pattern involves causing a buffer overflow through manipulation of environment variables. Once the adversary finds that they can modify an environment variable, they may try to overflow as...

- Server Side Include (SSI) Injection
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5
  Risk Scores: Financial: 2.24, Safety: 2.24, Privacy: 11.200000000000001
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: An attacker can use Server Side Include (SSI) Injection to send code to a web application that then gets executed by the web server. Doing so enables the attacker to achieve similar results to Cross S...

- Buffer Manipulation
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5
  Risk Scores: Financial: 2.24, Safety: 2.24, Privacy: 11.200000000000001
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: An adversary manipulates an application's interaction with a buffer in an attempt to read or modify data they shouldn't have access to. Buffer attacks are distinguished in that it is the buffer space ...

- Format String Injection
  Impact Scores: Financial: 1, Safety: 2.8, Privacy: 5
  Risk Scores: Financial: 2.24, Safety: 6.272, Privacy: 11.200000000000001
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: An adversary includes formatting characters in a string input field on the target application. Most applications assume that users will provide static text and may respond unpredictably to the presenc...

- Cache Poisoning
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5
  Risk Scores: Financial: 2.24, Safety: 2.24, Privacy: 11.200000000000001
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: An attacker exploits the functionality of cache technologies to cause specific data to be cached that aids the attackers' objectives. This describes any attack whereby an attacker places incorrect or ...

- DNS Cache Poisoning
  Impact Scores: Financial: 5, Safety: 1, Privacy: 1
  Risk Scores: Financial: 11.200000000000001, Safety: 2.24, Privacy: 2.24
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: A domain name server translates a domain name (such as www.example.com) into an IP address that Internet hosts use to contact Internet resources. An adversary modifies a public DNS cache to cause cert...

- Command Delimiters
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5
  Risk Scores: Financial: 2.24, Safety: 2.24, Privacy: 11.200000000000001
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: An attack of this type exploits a programs' vulnerabilities that allows an attacker's commands to be concatenated onto a legitimate command with the intent of targeting other resources such as the fil...

- Redirect Access to Libraries
  Impact Scores: Financial: 1, Safety: 5, Privacy: 1
  Risk Scores: Financial: 2.24, Safety: 11.200000000000001, Privacy: 2.24
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: An adversary exploits a weakness in the way an application searches for external libraries to manipulate the execution flow to point to an adversary supplied library or code base. This pattern of atta...

- XSS Targeting Non-Script Elements
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5
  Risk Scores: Financial: 2.24, Safety: 2.24, Privacy: 11.200000000000001
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: This attack is a form of Cross-Site Scripting (XSS) where malicious scripts are embedded in elements that are not expected to host scripts such as image tags (<img>), comments in XML documents (< !-CD...

- Malicious Automated Software Update via Redirection
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5
  Risk Scores: Financial: 2.24, Safety: 2.24, Privacy: 11.200000000000001
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: An attacker exploits two layers of weaknesses in server or client software for automated update mechanisms to undermine the integrity of the target code-base. The first weakness involves a failure to ...

- PHP Remote File Inclusion
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5
  Risk Scores: Financial: 2.24, Safety: 2.24, Privacy: 11.200000000000001
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: In this pattern the adversary is able to load and execute arbitrary code remotely available from the application. This is usually accomplished through an insecurely configured PHP runtime environment ...

- XSS Using Alternate Syntax
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5
  Risk Scores: Financial: 2.24, Safety: 2.24, Privacy: 11.200000000000001
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: An adversary uses alternate forms of keywords or commands that result in the same action as the primary form but which may not be caught by filters. For example, many keywords are processed in a case ...

- Serialized Data External Linking
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5
  Risk Scores: Financial: 2.24, Safety: 2.24, Privacy: 11.200000000000001
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: An adversary creates a serialized data file (e.g. XML, YAML, etc...) that contains an external data reference. Because serialized data parsers may not validate documents with external references, ther...

- Leveraging Race Conditions
  Impact Scores: Financial: 5, Safety: 1, Privacy: 1
  Risk Scores: Financial: 11.200000000000001, Safety: 2.24, Privacy: 2.24
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: The adversary targets a race condition occurring when multiple processes access and manipulate the same resource concurrently, and the outcome of the execution depends on the particular order in which...

- Leveraging Time-of-Check and Time-of-Use (TOCTOU) Race Conditions
  Impact Scores: Financial: 5, Safety: 1, Privacy: 1
  Risk Scores: Financial: 11.200000000000001, Safety: 2.24, Privacy: 2.24
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20

Description: This attack targets a race condition occurring between the time of check (state) for a resource and the time of use of a resource. A typical example is file access. The adversary can leverage a file a...

- Retrieve Embedded Sensitive Data
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5
  Risk Scores: Financial: 2.24, Safety: 2.24, Privacy: 11.200000000000001
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: An attacker examines a target system to find sensitive data that has been embedded within it. This information can reveal confidential contents, such as account numbers or individual keys/credentials ...

- Leveraging/Manipulating Configuration File Search Paths
  Impact Scores: Financial: 5, Safety: 1, Privacy: 1
  Risk Scores: Financial: 11.200000000000001, Safety: 2.24, Privacy: 2.24
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: This pattern of attack sees an adversary load a malicious resource into a program's standard path so that when a known command is executed then the system instead executes the malicious component. The...

- Manipulating Writeable Terminal Devices
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5
  Risk Scores: Financial: 2.24, Safety: 2.24, Privacy: 11.200000000000001
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: This attack exploits terminal devices that allow themselves to be written to by other users. The attacker sends command strings to the target terminal device hoping that the target user will hit enter...

- Using Meta-characters in E-mail Headers to Inject Malicious Payloads
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5
  Risk Scores: Financial: 2.24, Safety: 2.24, Privacy: 11.200000000000001
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: This type of attack involves an attacker leveraging meta-characters in email headers to inject improper behavior into email programs. Email software has become increasingly sophisticated and feature-r...

- Overflow Binary Resource File
  Impact Scores: Financial: 5, Safety: 1, Privacy: 1
  Risk Scores: Financial: 11.200000000000001, Safety: 2.24, Privacy: 2.24
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: An attack of this type exploits a buffer overflow vulnerability in the handling of binary resources. Binary resources may include music files like MP3, image files like JPEG files, and any other binar...

- Buffer Overflow via Symbolic Links
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5
  Risk Scores: Financial: 2.24, Safety: 2.24, Privacy: 11.200000000000001
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: This type of attack leverages the use of symbolic links to cause buffer overflows. An adversary can try to create or manipulate a symbolic link file such that its contents result in out of bounds data...

- Passing Local Filenames to Functions That Expect a URL
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5
  Risk Scores: Financial: 2.24, Safety: 2.24, Privacy: 11.200000000000001
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: This attack relies on client side code to access local files and resources instead of URLs. When the client browser is expecting a URL string, but instead receives a request for a local file, that exe...

- Poison Web Service Registry

Impact Scores: Financial: 1, Safety: 1, Privacy: 5
Risk Scores: Financial: 2.24, Safety: 2.24, Privacy: 11.200000000000001
Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
Description: SOA and Web Services often use a registry to perform look up, get schema information, and metadata about services. A poisoned registry can redirect (think phishing for servers) the service requester t...

- Session Credential Falsification through Prediction
  Impact Scores: Financial: 5, Safety: 1, Privacy: 1
  Risk Scores: Financial: 11.200000000000001, Safety: 2.24, Privacy: 2.24
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: This attack targets predictable session ID in order to gain privileges. The attacker can predict the session ID used during a transaction to perform spoofing and session hijacking....

- Using Slashes and URL Encoding Combined to Bypass Validation Logic
  Impact Scores: Financial: 5, Safety: 1, Privacy: 1
  Risk Scores: Financial: 11.200000000000001, Safety: 2.24, Privacy: 2.24
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: This attack targets the encoding of the URL combined with the encoding of the slash characters. An attacker can take advantage of the multiple ways of encoding a URL and abuse the interpretation of th...

- Voice Phishing
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5
  Risk Scores: Financial: 2.24, Safety: 2.24, Privacy: 11.200000000000001
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: An adversary targets users with a phishing attack for the purpose of soliciting account passwords or sensitive information from the user. Voice Phishing is a variation of the Phishing social engineeri...

- Malicious Automated Software Update via Spoofing
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5
  Risk Scores: Financial: 2.24, Safety: 2.24, Privacy: 11.200000000000001
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: An attackers uses identify or content spoofing to trick a client into performing an automated software update from a malicious source. A malicious automated software update that leverages spoofing can...

- String Format Overflow in syslog()
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5
  Risk Scores: Financial: 2.24, Safety: 2.24, Privacy: 11.200000000000001
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: This attack targets applications and software that uses the syslog() function insecurely. If an application does not explicitely use a format string parameter in a call to syslog(), user input can be ...

- Blind SQL Injection
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5
  Risk Scores: Financial: 2.24, Safety: 2.24, Privacy: 11.200000000000001
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: Blind SQL Injection results from an insufficient mitigation for SQL Injection. Although suppressing database error messages are considered best practice, the suppression alone is not sufficient to pre...

- URL Encoding
  Impact Scores: Financial: 5, Safety: 1, Privacy: 1
  Risk Scores: Financial: 11.200000000000001, Safety: 2.24, Privacy: 2.24
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: This attack targets the encoding of the URL. An adversary can take advantage of the multiple way of

encoding an URL and abuse the interpretation of the URL....

- User-Controlled Filename
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5
  Risk Scores: Financial: 2.24, Safety: 2.24, Privacy: 11.200000000000001
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: An attack of this type involves an adversary inserting malicious characters (such as a XSS redirection) into a filename, directly or indirectly that is then used by the target software to generate HTM...

- Manipulating User-Controlled Variables
  Impact Scores: Financial: 2.8, Safety: 1, Privacy: 5
  Risk Scores: Financial: 6.272, Safety: 2.24, Privacy: 11.200000000000001
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: This attack targets user controlled variables (DEBUG=1, PHP Globals, and So Forth). An adversary can override variables leveraging user-supplied, untrusted query variables directly used on the applica...

- Using Escaped Slashes in Alternate Encoding
  Impact Scores: Financial: 5, Safety: 1, Privacy: 1
  Risk Scores: Financial: 11.200000000000001, Safety: 2.24, Privacy: 2.24
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: This attack targets the use of the backslash in alternate encoding. An adversary can provide a backslash as a leading character and causes a parser to believe that the next character is special. This ...

- Buffer Overflow in an API Call
  Impact Scores: Financial: 5, Safety: 1, Privacy: 1
  Risk Scores: Financial: 11.200000000000001, Safety: 2.24, Privacy: 2.24
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: This attack targets libraries or shared code modules which are vulnerable to buffer overflow attacks. An adversary who has knowledge of known vulnerable libraries or shared code can easily target soft...

- Using UTF-8 Encoding to Bypass Validation Logic
  Impact Scores: Financial: 1, Safety: 5, Privacy: 1
  Risk Scores: Financial: 2.24, Safety: 11.200000000000001, Privacy: 2.24
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: This attack is a specific variation on leveraging alternate encodings to bypass validation logic. This attack leverages the possibility to encode potentially harmful input in UTF-8 and submit it to ap...

- XPath Injection
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5
  Risk Scores: Financial: 2.24, Safety: 2.24, Privacy: 11.200000000000001
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: An attacker can craft special user-controllable input consisting of XPath expressions to inject the XML database and bypass authentication or glean information that they normally would not be able to....

- XQuery Injection
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5
  Risk Scores: Financial: 2.24, Safety: 2.24, Privacy: 11.200000000000001
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: This attack utilizes XQuery to probe and attack server systems; in a similar manner that SQL Injection allows an attacker to exploit SQL calls to RDBMS, XQuery Injection uses improperly validated data...

- OS Command Injection
  Impact Scores: Financial: 5, Safety: 1, Privacy: 1

Risk Scores: Financial: 11.200000000000001, Safety: 2.24, Privacy: 2.24
Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
Description: In this type of an attack, an adversary injects operating system commands into existing application functions. An application that uses untrusted input to build command strings is vulnerable. An adver...

- Pharming
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5
  Risk Scores: Financial: 2.24, Safety: 2.24, Privacy: 11.200000000000001
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: A pharming attack occurs when the victim is fooled into entering sensitive data into supposedly trusted locations, such as an online bank site or a trading platform. An attacker can impersonate these ...

- Buffer Overflow in Local Command-Line Utilities
  Impact Scores: Financial: 5, Safety: 1, Privacy: 1
  Risk Scores: Financial: 11.200000000000001, Safety: 2.24, Privacy: 2.24
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: This attack targets command-line utilities available in a number of shells. An adversary can leverage a vulnerability found in a command-line utility to escalate privilege to root....

- Reflection Attack in Authentication Protocol
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5
  Risk Scores: Financial: 2.24, Safety: 2.24, Privacy: 11.200000000000001
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: An adversary can abuse an authentication protocol susceptible to reflection attack in order to defeat it. Doing so allows the adversary illegitimate access to the target system, without possessing the...

- Forced Integer Overflow
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5
  Risk Scores: Financial: 2.24, Safety: 2.24, Privacy: 11.200000000000001
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: This attack forces an integer variable to go out of range. The integer variable is often used as an offset such as size of memory allocation or similarly. The attacker would typically control the valu...

- WSDL Scanning
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5
  Risk Scores: Financial: 2.24, Safety: 2.24, Privacy: 11.200000000000001
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: This attack targets the WSDL interface made available by a web service. The attacker may scan the WSDL interface to reveal sensitive information about invocation patterns, underlying technology implem...

- Phishing
  Impact Scores: Financial: 1.4, Safety: 1, Privacy: 5
  Risk Scores: Financial: 3.136, Safety: 2.24, Privacy: 11.200000000000001
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: Phishing is a social engineering technique where an attacker masquerades as a legitimate entity with which the victim might do business in order to prompt the user to reveal some confidential informat...

- Flooding
  Impact Scores: Financial: 1, Safety: 1.4, Privacy: 4.199999999999999
  Risk Scores: Financial: 2.24, Safety: 3.136, Privacy: 9.408
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: An adversary consumes the resources of a target by rapidly engaging in a large number of interactions with the target. This type of attack generally exposes a weakness in rate limiting or flow. When s...

- Directory Indexing
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.199999999999999
  Risk Scores: Financial: 2.24, Safety: 2.24, Privacy: 9.408
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: An adversary crafts a request to a target that results in the target listing/indexing the content of a directory as output. One common method of triggering directory contents as output is to construct...

- Flash Parameter Injection
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.199999999999999
  Risk Scores: Financial: 2.24, Safety: 2.24, Privacy: 9.408
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: An adversary takes advantage of improper data validation to inject malicious global parameters into a Flash file embedded within an HTML document. Flash files can leverage user-submitted data to confi...

- Exploiting Incorrectly Configured Access Control Security Levels
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.199999999999999
  Risk Scores: Financial: 2.24, Safety: 2.24, Privacy: 9.408
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: An attacker exploits a weakness in the configuration of access controls and is able to bypass the intended protection that these measures guard against and thereby obtain unauthorized access to the sy...

- Exponential Data Expansion
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.199999999999999
  Risk Scores: Financial: 2.24, Safety: 2.24, Privacy: 9.408
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: An adversary submits data to a target application which contains nested exponential data expansion to produce excessively large output. Many data format languages allow the definition of macro-like st...

- Inducing Account Lockout
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.199999999999999
  Risk Scores: Financial: 2.24, Safety: 2.24, Privacy: 9.408
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: An attacker leverages the security functionality of the system aimed at thwarting potential attacks to launch a denial of service attack against a legitimate system user. Many systems, for instance, i...

- XML Routing Detour Attacks
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.199999999999999
  Risk Scores: Financial: 2.24, Safety: 2.24, Privacy: 9.408
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: An attacker subverts an intermediate system used to process XML content and forces the intermediate to modify and/or re-route the processing of the content. XML Routing Detour Attacks are Adversary in...

- Fuzzing
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.199999999999999
  Risk Scores: Financial: 2.24, Safety: 2.24, Privacy: 9.408
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: In this attack pattern, the adversary leverages fuzzing to try to identify weaknesses in the system. Fuzzing is a software security and functionality testing method that feeds randomly constructed inp...

- Manipulating Opaque Client-based Data Tokens
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.199999999999999
  Risk Scores: Financial: 2.24, Safety: 2.24, Privacy: 9.408
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20

Description: In circumstances where an application holds important data client-side in tokens (cookies, URLs, data files, and so forth) that data can be manipulated. If client or server-side application components...

- CAN Injection
  Impact Scores: Financial: 4.199999999999999, Safety: 5, Privacy: 2.8
  Risk Scores: Financial: 7.055999999999999, Safety: 8.4, Privacy: 4.704
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: Manipulation of CAN bus messages leading to vehicle malfunction...

- HTTP Request Splitting
  Impact Scores: Financial: 5, Safety: 1, Privacy: 1
  Risk Scores: Financial: 8.4, Safety: 1.6800000000000002, Privacy: 1.6800000000000002
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: An adversary abuses the flexibility and discrepancies in the parsing and interpretation of HTTP Request messages by different intermediary HTTP agents (e.g., load balancer, reverse proxy, web caching ...

- Serialized Data with Nested Payloads
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5
  Risk Scores: Financial: 1.6800000000000002, Safety: 1.6800000000000002, Privacy: 8.4
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: Applications often need to transform data in and out of a data format (e.g., XML and YAML) by using a parser. It may be possible for an adversary to inject data that may have an adverse effect on the ...

- Command Injection
  Impact Scores: Financial: 5, Safety: 1, Privacy: 1
  Risk Scores: Financial: 8.4, Safety: 1.6800000000000002, Privacy: 1.6800000000000002
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: An adversary looking to execute a command of their choosing, injects new items into an existing command thus modifying interpretation away from what was intended. Commands in this context are often st...

- Leveraging Race Conditions via Symbolic Links
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5
  Risk Scores: Financial: 1.6800000000000002, Safety: 1.6800000000000002, Privacy: 8.4
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: This attack leverages the use of symbolic links (Symlinks) in order to write to sensitive files. An attacker can create a Symlink link to a target file not otherwise accessible to them. When the privi...

- HTTP Response Smuggling
  Impact Scores: Financial: 5, Safety: 1, Privacy: 1
  Risk Scores: Financial: 8.4, Safety: 1.6800000000000002, Privacy: 1.6800000000000002
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: An adversary manipulates and injects malicious content in the form of secret unauthorized HTTP responses, into a single HTTP response from a vulnerable or compromised back-end HTTP agent (e.g., server...

- SOAP Manipulation
  Impact Scores: Financial: 5, Safety: 1, Privacy: 1
  Risk Scores: Financial: 8.4, Safety: 1.6800000000000002, Privacy: 1.6800000000000002
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: Simple Object Access Protocol (SOAP) is used as a communication protocol between a client and server to invoke web services on the server. It is an XML-based protocol, and therefore suffers from many ...

- HTTP Request Smuggling
  Impact Scores: Financial: 5, Safety: 1, Privacy: 1

Risk Scores: Financial: 8.4, Safety: 1.6800000000000002, Privacy: 1.6800000000000002
Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
Description: An adversary abuses the flexibility and discrepancies in the parsing and interpretation of HTTP Request messages using various HTTP headers, request-line and body parameters as well as message sizes (...

- HTTP Response Splitting
  Impact Scores: Financial: 5, Safety: 1, Privacy: 1
  Risk Scores: Financial: 8.4, Safety: 1.6800000000000002, Privacy: 1.6800000000000002
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: An adversary manipulates and injects malicious content, in the form of secret unauthorized HTTP responses, into a single HTTP response from a vulnerable or compromised back-end HTTP agent (e.g., web s...

- Using Alternative IP Address Encodings
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5
  Risk Scores: Financial: 1.6800000000000002, Safety: 1.6800000000000002, Privacy: 8.4
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: This attack relies on the adversary using unexpected formats for representing IP addresses. Networked applications may expect network location information in a specific format, such as fully qualified...

- Exploiting Multiple Input Interpretation Layers
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5
  Risk Scores: Financial: 1.6800000000000002, Safety: 1.6800000000000002, Privacy: 8.4
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: An attacker supplies the target software with input data that contains sequences of special characters designed to bypass input validation logic. This exploit relies on the target making multiples pas...

- Development Alteration
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5
  Risk Scores: Financial: 1.6800000000000002, Safety: 1.6800000000000002, Privacy: 8.4
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: An adversary modifies a technology, product, or component during its development to acheive a negative impact once the system is deployed. The goal of the adversary is to modify the system in such a w...

- Malicious Logic Insertion into Product Software via Configuration Management Manipulation
  Impact Scores: Financial: 5, Safety: 1, Privacy: 1
  Risk Scores: Financial: 8.4, Safety: 1.6800000000000002, Privacy: 1.6800000000000002
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: An adversary exploits a configuration management system so that malicious logic is inserted into a software products build, update or deployed environment. If an adversary can control the elements inc...

- Design Alteration
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5
  Risk Scores: Financial: 1.6800000000000002, Safety: 1.6800000000000002, Privacy: 8.4
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: An adversary modifies the design of a technology, product, or component to acheive a negative impact once the system is deployed. In this type of attack, the goal of the adversary is to modify the des...

- Contradictory Destinations in Traffic Routing Schemes
  Impact Scores: Financial: 5, Safety: 1, Privacy: 1
  Risk Scores: Financial: 8.4, Safety: 1.6800000000000002, Privacy: 1.6800000000000002
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: Adversaries can provide contradictory destinations when sending messages. Traffic is routed in networks using the domain names in various headers available at different levels of the OSI model. In a C...

- Object Injection
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5
  Risk Scores: Financial: 1.6800000000000002, Safety: 1.6800000000000002, Privacy: 8.4
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: An adversary attempts to exploit an application by injecting additional, malicious content during its processing of serialized objects. Developers leverage serialization in order to convert data or st...

- Root/Jailbreak Detection Evasion via Debugging
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5
  Risk Scores: Financial: 1.6800000000000002, Safety: 1.6800000000000002, Privacy: 8.4
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: An adversary inserts a debugger into the program entry point of a mobile application to modify the application binary, with the goal of evading Root/Jailbreak detection. Mobile device users often Root...

- Bluetooth Impersonation AttackS (BIAS)
  Impact Scores: Financial: 5, Safety: 1, Privacy: 1
  Risk Scores: Financial: 8.4, Safety: 1.6800000000000002, Privacy: 1.6800000000000002
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: An adversary disguises the MAC address of their Bluetooth enabled device to one for which there exists an active and trusted connection and authenticates successfully. The adversary can then perform m...

- Alteration of a Software Update
  Impact Scores: Financial: 5, Safety: 1, Privacy: 1
  Risk Scores: Financial: 8.4, Safety: 1.6800000000000002, Privacy: 1.6800000000000002
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: An adversary with access to an organization’s software update infrastructure inserts malware into the content of an outgoing update to fielded systems where a wide range of malicious effects are possi...

- Eavesdropping on a Monitor
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5
  Risk Scores: Financial: 1.6800000000000002, Safety: 1.6800000000000002, Privacy: 8.4
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: An Adversary can eavesdrop on the content of an external monitor through the air without modifying any cable or installing software, just capturing this signal emitted by the cable or video port, with...

- Browser in the Middle (BiTM)
  Impact Scores: Financial: 5, Safety: 1, Privacy: 1
  Risk Scores: Financial: 8.4, Safety: 1.6800000000000002, Privacy: 1.6800000000000002
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: An adversary exploits the inherent functionalities of a web browser, in order to establish an unnoticed remote desktop connection in the victim's browser to the adversary's system. The adversary must ...

- Manipulating State
  Impact Scores: Financial: 1.4, Safety: 1, Privacy: 5
  Risk Scores: Financial: 2.352, Safety: 1.6800000000000002, Privacy: 8.4
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: The adversary modifies state information maintained by the target software or causes a state transition in hardware. If successful, the target will use this tainted state and execute in an unintended ...

- Interface Manipulation
  Impact Scores: Financial: 4.199999999999999, Safety: 1, Privacy: 1
  Risk Scores: Financial: 7.055999999999999, Safety: 1.6800000000000002, Privacy: 1.6800000000000002
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20

Description: An adversary manipulates the use or processing of an interface (e.g. Application Programming Interface (API) or System-on-Chip (SoC)) resulting in an adverse impact upon the security of the system imp...

- Parameter Injection
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.199999999999999
  Risk Scores: Financial: 1.6800000000000002, Safety: 1.6800000000000002, Privacy: 7.055999999999999
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: An adversary manipulates the content of request parameters for the purpose of undermining the security of the target. Some parameter encodings use text characters as separators. For example, parameter...

- Content Spoofing
  Impact Scores: Financial: 4.199999999999999, Safety: 1, Privacy: 4.199999999999999
  Risk Scores: Financial: 7.055999999999999, Safety: 1.6800000000000002, Privacy: 7.055999999999999
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: An adversary modifies content to make it contain something other than what the original content producer intended while keeping the apparent source of the content unchanged. The term content spoofing ...

- Resource Location Spoofing
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.199999999999999
  Risk Scores: Financial: 1.6800000000000002, Safety: 1.6800000000000002, Privacy: 7.055999999999999
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: An adversary deceives an application or user and convinces them to request a resource from an unintended location. By spoofing the location, the adversary can cause an alternate resource to be used, o...

- Cross-Site Flashing
  Impact Scores: Financial: 4.199999999999999, Safety: 1, Privacy: 1
  Risk Scores: Financial: 7.055999999999999, Safety: 1.6800000000000002, Privacy: 1.6800000000000002
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: An attacker is able to trick the victim into executing a Flash document that passes commands or calls to a Flash player browser plugin, allowing the attacker to exploit native Flash functionality in t...

- Modification of Registry Run Keys
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.199999999999999
  Risk Scores: Financial: 1.6800000000000002, Safety: 1.6800000000000002, Privacy: 7.055999999999999
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: An adversary adds a new entry to the run keys in the Windows registry so that an application of their choosing is executed when a user logs in. In this way, the adversary can get their executable to o...

- Using Leading 'Ghost' Character Sequences to Bypass Input Filters
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.199999999999999
  Risk Scores: Financial: 1.6800000000000002, Safety: 1.6800000000000002, Privacy: 7.055999999999999
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: Some APIs will strip certain leading characters from a string of parameters. An adversary can intentionally introduce leading ghost characters (extra characters that don't affect the validity of the r...

- Manipulate Human Behavior
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.199999999999999
  Risk Scores: Financial: 1.6800000000000002, Safety: 1.6800000000000002, Privacy: 7.055999999999999
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: An adversary exploits inherent human psychological predisposition to influence a targeted individual or group to solicit information or manipulate the target into performing an action that serves the ...

- Disable Security Software

Impact Scores: Financial: 4.199999999999999, Safety: 1, Privacy: 1
Risk Scores: Financial: 7.055999999999999, Safety: 1.6800000000000002, Privacy: 1.6800000000000002
Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
Description: An adversary exploits a weakness in access control to disable security tools so that detection does not occur. This can take the form of killing processes, deleting registry keys so that tools do not ...

- Collect Data from Registries
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.199999999999999
  Risk Scores: Financial: 1.6800000000000002, Safety: 1.6800000000000002, Privacy: 7.055999999999999
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: An adversary exploits a weakness in authorization to gather system-specific data and sensitive information within a registry (e.g., Windows Registry, Mac plist). These contain information about the sy...

- Collect Data from Screen Capture
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.199999999999999
  Risk Scores: Financial: 1.6800000000000002, Safety: 1.6800000000000002, Privacy: 7.055999999999999
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: An adversary gathers sensitive information by exploiting the system's screen capture functionality. Through screenshots, the adversary aims to see what happens on the screen over the course of an oper...

- Retrieve Data from Decommissioned Devices
  Impact Scores: Financial: 1, Safety: 1.4, Privacy: 4.199999999999999
  Risk Scores: Financial: 1.6800000000000002, Safety: 2.352, Privacy: 7.055999999999999
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: An adversary obtains decommissioned, recycled, or discarded systems and devices that can include an organization’s intellectual property, employee data, and other types of controlled information. Syst...

- Web Application Fingerprinting
  Impact Scores: Financial: 1, Safety: 1, Privacy: 2.8
  Risk Scores: Financial: 2.24, Safety: 2.24, Privacy: 6.272
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: An attacker sends a series of probes to a web application in order to elicit version-dependent and type-dependent behavior that assists in identifying the target. An attacker could learn information s...

- Fuzzing for application mapping
  Impact Scores: Financial: 1, Safety: 2.8, Privacy: 1
  Risk Scores: Financial: 2.24, Safety: 6.272, Privacy: 2.24
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: An attacker sends random, malformed, or otherwise unexpected messages to a target application and observes the application's log or error messages returned. The attacker does not initially know how a ...

- AJAX Footprinting
  Impact Scores: Financial: 1, Safety: 1, Privacy: 2.8
  Risk Scores: Financial: 2.24, Safety: 2.24, Privacy: 6.272
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: This attack utilizes the frequent client-server roundtrips in Ajax conversation to scan a system. While Ajax does not open up new vulnerabilities per se, it does optimize them from an attacker point o...

- Escaping a Sandbox by Calling Code in Another Language
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5
  Risk Scores: Financial: 1.12, Safety: 1.12, Privacy: 5.6000000000000005
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: The attacker may submit malicious code of another language to obtain access to privileges that were not

intentionally exposed by the sandbox, thus escaping the sandbox. For instance, Java code cannot ...

- Forced Deadlock
  Impact Scores: Financial: 5, Safety: 1, Privacy: 1
  Risk Scores: Financial: 5.6000000000000005, Safety: 1.12, Privacy: 1.12
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: The adversary triggers and exploits a deadlock condition in the target software to cause a denial of service. A deadlock can occur when two or more competing actions are waiting for each other to fini...

- Schema Poisoning
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5
  Risk Scores: Financial: 1.12, Safety: 1.12, Privacy: 5.6000000000000005
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: An adversary corrupts or modifies the content of a schema for the purpose of undermining the security of the target. Schemas provide the structure and content definitions for resources used by an appl...

- Hijacking a Privileged Thread of Execution
  Impact Scores: Financial: 5, Safety: 1, Privacy: 1
  Risk Scores: Financial: 5.6000000000000005, Safety: 1.12, Privacy: 1.12
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: An adversary hijacks a privileged thread of execution by injecting malicious code into a running process. By using a privleged thread to do their bidding, adversaries can evade process-based detection...

- USB Memory Attacks
  Impact Scores: Financial: 2.8, Safety: 1, Privacy: 5
  Risk Scores: Financial: 3.136, Safety: 1.12, Privacy: 5.6000000000000005
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: An adversary loads malicious code onto a USB memory stick in order to infect any system which the device is plugged in to. USB drives present a significant security risk for business and government ag...

- Signature Spoofing by Misrepresentation
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5
  Risk Scores: Financial: 1.12, Safety: 1.12, Privacy: 5.6000000000000005
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: An attacker exploits a weakness in the parsing or display code of the recipient software to generate a data blob containing a supposedly valid signature, but the signer's identity is falsely represent...

- Hardware Component Substitution During Baselining
  Impact Scores: Financial: 5, Safety: 1, Privacy: 1
  Risk Scores: Financial: 5.6000000000000005, Safety: 1.12, Privacy: 1.12
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: An adversary with access to system components during allocated baseline development can substitute a maliciously altered hardware component for a baseline component during the product development and ...

- Malicious Hardware Update
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5
  Risk Scores: Financial: 1.12, Safety: 1.12, Privacy: 5.6000000000000005
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: An adversary introduces malicious hardware during an update or replacement procedure, allowing for additional compromise or site disruption at the victim location. After deployment, it is not uncommon...

- Open-Source Library Manipulation
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5

Risk Scores: Financial: 1.12, Safety: 1.12, Privacy: 5.6000000000000005
Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
Description: Adversaries implant malicious code in open source software (OSS) libraries to have it widely distributed, as OSS is commonly downloaded by developers and other users to incorporate into software devel...

- ASIC With Malicious Functionality
Impact Scores: Financial: 5, Safety: 1, Privacy: 1
Risk Scores: Financial: 5.6000000000000005, Safety: 1.12, Privacy: 1.12
Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
Description: An attacker with access to the development environment process of an application-specific integrated circuit (ASIC) for a victim system being developed or maintained after initial deployment can inser...

- Hardware Fault Injection
Impact Scores: Financial: 1, Safety: 5, Privacy: 5
Risk Scores: Financial: 1.12, Safety: 5.6000000000000005, Privacy: 5.6000000000000005
Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
Description: The adversary uses disruptive signals or events, or alters the physical environment a device operates in, to cause faulty behavior in electronic devices. This can include electromagnetic pulses, laser...

- Carry-Off GPS Attack
Impact Scores: Financial: 1, Safety: 1, Privacy: 5
Risk Scores: Financial: 1.12, Safety: 1.12, Privacy: 5.6000000000000005
Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
Description: A common form of a GPS spoofing attack, commonly termed a carry-off attack begins with an adversary broadcasting signals synchronized with the genuine signals observed by the target receiver. The powe...

- DLL Side-Loading
Impact Scores: Financial: 1, Safety: 1, Privacy: 5
Risk Scores: Financial: 1.12, Safety: 1.12, Privacy: 5.6000000000000005
Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
Description: An adversary places a malicious version of a Dynamic-Link Library (DLL) in the Windows Side-by-Side (WinSxS) directory to trick the operating system into loading this malicious DLL instead of a legiti...

- Use of Captured Tickets (Pass The Ticket)
Impact Scores: Financial: 1, Safety: 1, Privacy: 5
Risk Scores: Financial: 1.12, Safety: 1.12, Privacy: 5.6000000000000005
Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
Description: An adversary uses stolen Kerberos tickets to access systems/resources that leverage the Kerberos authentication protocol. The Kerberos authentication protocol centers around a ticketing system which i...

- Sniff Application Code
Impact Scores: Financial: 1, Safety: 1, Privacy: 5
Risk Scores: Financial: 1.12, Safety: 1.12, Privacy: 5.6000000000000005
Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
Description: An adversary passively sniffs network communications and captures application code bound for an authorized client. Once obtained, they can use it as-is, or through reverse-engineering glean sensitive ...

- Key Negotiation of Bluetooth Attack (KNOB)
Impact Scores: Financial: 1, Safety: 1, Privacy: 5
Risk Scores: Financial: 1.12, Safety: 1.12, Privacy: 5.6000000000000005
Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
Description: An adversary can exploit a flaw in Bluetooth key negotiation allowing them to decrypt information sent between two devices communicating via Bluetooth. The adversary uses an Adversary in the Middle se...

- Malicious Code Implanted During Chip Programming
  Impact Scores: Financial: 5, Safety: 1, Privacy: 1
  Risk Scores: Financial: 5.6000000000000005, Safety: 1.12, Privacy: 1.12
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: During the programming step of chip manufacture, an adversary with access and necessary technical skills maliciously alters a chip’s intended program logic to produce an effect intended by the adversa...

- Subvert Code-signing Facilities
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5
  Risk Scores: Financial: 1.12, Safety: 1.12, Privacy: 5.6000000000000005
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: Many languages use code signing facilities to vouch for code's identity and to thus tie code to its assigned privileges within an environment. Subverting this mechanism can be instrumental in an attac...

- Load Value Injection
  Impact Scores: Financial: 1, Safety: 1, Privacy: 5
  Risk Scores: Financial: 1.12, Safety: 1.12, Privacy: 5.6000000000000005
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: An adversary exploits a hardware design flaw in a CPU implementation of transient instruction execution in which a faulting or assisted load instruction transiently forwards adversary-controlled data ...

- Interception
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.199999999999999
  Risk Scores: Financial: 1.12, Safety: 1.12, Privacy: 4.704
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: An adversary monitors data streams to or from the target for information gathering purposes. This attack may be undertaken to solely gather sensitive information or to support a further attack against...

- XML Ping of the Death
  Impact Scores: Financial: 1, Safety: 4.199999999999999, Privacy: 1
  Risk Scores: Financial: 1.12, Safety: 4.704, Privacy: 1.12
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: An attacker initiates a resource depletion attack where a large number of small XML messages are delivered at a sufficiently rapid rate to cause a denial of service or crash of the target. Transaction...

- Active OS Fingerprinting
  Impact Scores: Financial: 1, Safety: 1, Privacy: 2.8
  Risk Scores: Financial: 1.6800000000000002, Safety: 1.6800000000000002, Privacy: 4.704
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: An adversary engages in activity to detect the operating system or firmware version of a remote target by interrogating a device, server, or platform with a probe designed to solicit behavior that wil...

- TCP Timestamp Probe
  Impact Scores: Financial: 2.8, Safety: 1, Privacy: 1
  Risk Scores: Financial: 4.704, Safety: 1.6800000000000002, Privacy: 1.6800000000000002
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: This OS fingerprinting probe examines the remote server's implementation of TCP timestamps. Not all operating systems implement timestamps within the TCP header, but when timestamps are used then this...

- TCP Sequence Number Probe
  Impact Scores: Financial: 2.8, Safety: 1, Privacy: 1
  Risk Scores: Financial: 4.704, Safety: 1.6800000000000002, Privacy: 1.6800000000000002
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20

Description: This OS fingerprinting probe tests the target system's assignment of TCP sequence numbers. One common way to test TCP Sequence Number generation is to send a probe packet to an open port on the target...

- TCP (ISN) Greatest Common Divisor Probe
  Impact Scores: Financial: 1, Safety: 1, Privacy: 2.8
  Risk Scores: Financial: 1.6800000000000002, Safety: 1.6800000000000002, Privacy: 4.704
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: This OS fingerprinting probe sends a number of TCP SYN packets to an open port of a remote machine. The Initial Sequence Number (ISN) in each of the SYN/ACK response packets is analyzed to determine t...

- TCP (ISN) Counter Rate Probe
  Impact Scores: Financial: 1, Safety: 1, Privacy: 2.8
  Risk Scores: Financial: 1.6800000000000002, Safety: 1.6800000000000002, Privacy: 4.704
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: This OS detection probe measures the average rate of initial sequence number increments during a period of time. Sequence numbers are incremented using a time-based algorithm and are susceptible to a ...

- TCP (ISN) Sequence Predictability Probe
  Impact Scores: Financial: 1, Safety: 1, Privacy: 2.8
  Risk Scores: Financial: 1.6800000000000002, Safety: 1.6800000000000002, Privacy: 4.704
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: This type of operating system probe attempts to determine an estimate for how predictable the sequence number generation algorithm is for a remote host. Statistical techniques, such as standard deviat...

- TCP Initial Window Size Probe
  Impact Scores: Financial: 2.8, Safety: 1, Privacy: 1
  Risk Scores: Financial: 4.704, Safety: 1.6800000000000002, Privacy: 1.6800000000000002
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: This OS fingerprinting probe checks the initial TCP Window size. TCP stacks limit the range of sequence numbers allowable within a session to maintain the connected state within TCP protocol logic. Th...

- TCP Options Probe
  Impact Scores: Financial: 2.8, Safety: 1, Privacy: 1
  Risk Scores: Financial: 4.704, Safety: 1.6800000000000002, Privacy: 1.6800000000000002
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: This OS fingerprinting probe analyzes the type and order of any TCP header options present within a response segment. Most operating systems use unique ordering and different option sets when options ...

- Pretexting
  Impact Scores: Financial: 1, Safety: 1, Privacy: 2.8
  Risk Scores: Financial: 1.6800000000000002, Safety: 1.6800000000000002, Privacy: 4.704
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: An adversary engages in pretexting behavior to solicit information from target persons, or manipulate the target into performing some action that serves the adversary's interests. During a pretexting ...

- Incomplete Data Deletion in a Multi-Tenant Environment
  Impact Scores: Financial: 1, Safety: 1, Privacy: 4.199999999999999
  Risk Scores: Financial: 1.12, Safety: 1.12, Privacy: 4.704
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: An adversary obtains unauthorized information due to insecure or incomplete data deletion in a multi-tenant environment. If a cloud provider fails to completely delete storage and data from former clo...

- Adding a Space to a File Extension

Impact Scores: Financial: 1, Safety: 1, Privacy: 4.199999999999999
Risk Scores: Financial: 1.12, Safety: 1.12, Privacy: 4.704
Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
Description: An adversary adds a space character to the end of a file extension and takes advantage of an application that does not properly neutralize trailing special elements in file names. This extra space, wh...

- Reverse Engineering
  Impact Scores: Financial: 2.8, Safety: 1, Privacy: 1
  Risk Scores: Financial: 3.136, Safety: 1.12, Privacy: 1.12
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: An adversary discovers the structure, function, and composition of an object, resource, or system by using a variety of analysis techniques to effectively determine how the analyzed entity was constru...

- Fingerprinting
  Impact Scores: Financial: 1, Safety: 1, Privacy: 1.4
  Risk Scores: Financial: 2.24, Safety: 2.24, Privacy: 3.136
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: An adversary compares output from a target system to known indicators that uniquely identify specific details about the target. Most commonly, fingerprinting is done to determine operating system and ...

- Target Influence via Framing
  Impact Scores: Financial: 1, Safety: 1.4, Privacy: 2.8
  Risk Scores: Financial: 1.12, Safety: 1.568, Privacy: 3.136
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: An adversary uses framing techniques to contextualize a conversation so that the target is more likely to be influenced by the adversary's point of view. Framing is information and experiences in life...

- Influence via Psychological Principles
  Impact Scores: Financial: 2.8, Safety: 1, Privacy: 1
  Risk Scores: Financial: 3.136, Safety: 1.12, Privacy: 1.12
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: The adversary shapes the target's actions or behavior by focusing on the ways human interact and learn, leveraging such elements as cognitive and social psychology. In a variety of ways, a target can ...

- Process Footprinting
  Impact Scores: Financial: 1, Safety: 1, Privacy: 2.8
  Risk Scores: Financial: 1.12, Safety: 1.12, Privacy: 3.136
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: An adversary exploits functionality meant to identify information about the currently running processes on the target system to an authorized user. By knowing what processes are running on the target ...

- Services Footprinting
  Impact Scores: Financial: 1, Safety: 1, Privacy: 2.8
  Risk Scores: Financial: 1.12, Safety: 1.12, Privacy: 3.136
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: An adversary exploits functionality meant to identify information about the services on the target system to an authorized user. By knowing what services are registered on the target system, the adver...

- Account Footprinting
  Impact Scores: Financial: 1, Safety: 1, Privacy: 2.8
  Risk Scores: Financial: 1.12, Safety: 1.12, Privacy: 3.136
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: An adversary exploits functionality meant to identify information about the domain accounts and their

permissions on the target system to an authorized user. By knowing what accounts are registered on...

- Group Permission Footprinting
  Impact Scores: Financial: 1, Safety: 1, Privacy: 2.8
  Risk Scores: Financial: 1.12, Safety: 1.12, Privacy: 3.136
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: An adversary exploits functionality meant to identify information about user groups and their permissions on the target system to an authorized user. By knowing what users/permissions are registered o...

- Owner Footprinting
  Impact Scores: Financial: 1, Safety: 1, Privacy: 2.8
  Risk Scores: Financial: 1.12, Safety: 1.12, Privacy: 3.136
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: An adversary exploits functionality meant to identify information about the primary users on the target system to an authorized user. They may do this, for example, by reviewing logins or file modific...

- System Footprinting
  Impact Scores: Financial: 1, Safety: 1, Privacy: 2.8
  Risk Scores: Financial: 1.12, Safety: 1.12, Privacy: 3.136
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: An adversary engages in active probing and exploration activities to determine security information about a remote target system. Often times adversaries will rely on remote applications that can be p...

- Collect Data from Clipboard
  Impact Scores: Financial: 1, Safety: 1, Privacy: 2.8
  Risk Scores: Financial: 1.12, Safety: 1.12, Privacy: 3.136
  Risk Factors: exposure: 0.50, complexity: 0.30, attack_surface: 0.20
  Description: The adversary exploits an application that allows for the copying of sensitive data or information by collecting information copied to the clipboard. Data copied to the clipboard can be accessed by ot...