Device: Mitsubishi Electric smartRTU
EPSS Score: 0.000810000
CVSS Score: 6.1
CVSS Severity: MEDIUM

CVE ID: CVE-2018-16061

Attack ID: T1027
Description: Obfuscated Files or Information
Score: 0.07372624368502757

Application Isolation and Sandboxing (ID: M1048)

D3-DA Dynamic Analysis

Definition: Executing or opening a file in a synthetic "sandbox" environment to determine if the file is a malicious program or if the file exploits another program such as a document reader.
How it works: Analyzing the interaction of a piece of code with a system while the code is being executed in a controlled environment such as a sandbox, virtual machine, or simulator. This exposes the natural behavior of the piece of code without requiring the code to be disassembled.
Considerations: Malware often detects a fake environment, then changes its behavior accordingly. For example, it could detect that the system clock is being sped up in an effort to get it to execute commands that it would normally only execute at a later time, or that the hardware manufacturer of the machine is a virtualization Provider, Malware can attempt to determine if it is being debugged, and change its behavior accordingly, Sometimes the malware behavior is triggered only under certain conditions (on a specific system date, after a certain time, or after it is sent a specific command) and can't be detected through a short execution in a virtual environment.
Implementations: Cuckoo Sandbox
Examples: No examples available

D3-HBPI Hardware-based Process Isolation

Definition: Preventing one process from writing to the memory space of another process through hardware based address manager implementations.
How it works: Process isolation, in this context, is address space separation controlled by a security function that limits the communication between processes so that one process cannot directly modify the executing code of another process. Hardware process isolation is commonly implemented through Direct Memory Access (DMA) which collaborates with a Memory Management Unit (MMU), or Input-Output Memory Management Unit (IOMMU). These hardware controls are deployed directly on processors to aid hosts or enclaves in process isolation.
Considerations: Private hosts may be vulnerable to DMA attack if they have a PCI or PCI Express port that connects attached devices directly to physical address space.
Implementations: Intel Virtualization Technology for Directed I/O (Intel VT-d), Firecracker
Examples: No examples available

D3-MAC Mandatory Access Control

Definition: Controlling access to local computer system resources with kernel-level capabilities.
How it works: Mandatory access control is a non-discretionary access control system because the rules and polices that determine access is determined by a security control authority and not distributed to local users. Access determinations are based on designed access control polices and are not based on local resource owner determinations. Access is typically granted by defining sets of subjects and sets of objects. Subjects are the entities requesting access and objects are the resources that subjects are trying to access. Rules and policies are defined that associate subjects and object permissions and access controls.
Considerations: None
Implementations: Some implementations of security label mandatory access control contain complex rules set that are hard to verify and complex to maintain over time. Initial planning of access model and continuous monitoring of the available users, resources and object is necessary
Examples: Linux C-Groups, and Policy engines like SELinux, Windows Mandatory Integrity Control introduced in Windows Vista

D3-SCF System Call Filtering

No additional information available