

Device: Rockwell Automation MicroLogix 1400 Controllers Series B
EPSS Score: 0.000580000
CVSS Score: 9.8
CVSS Severity: CRITICAL

CVE ID: CVE-2017-7899

Attack ID: T1185
Description: Browser Session Hijacking
Score: 0.13164525388328563

User Training (ID: M1017)

User Account Management (ID: M1018)

No Defense Measure
Reason: Modeling user training is outside the scope of D3FEND.

D3-LFP Local File Permissions

D3-MAC Mandatory Access Control

D3-SCP System Configuration Permissions

No additional information available

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 policies that determine access is determined by a security control authority and not distributed to local users. Access determinations are based on designed access control policies 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

No additional information available