# Application Isolation and Sandboxing, Mitigation M0948 - ICS

By Authorization Enforcement

Archived: 2026-04-05 18:01:50 UTC

| Domain | ID | Name | Use |
|---|---|---|---|
| ICS | T0817 | Drive-by Compromise | Built-in browser sandboxes and application isolation may be used to contain web-based malware. |
| ICS | T0819 | Exploit Public-Facing Application | Application isolation will limit the other processes and system features an exploited target can access. Examples of built in features are software restriction policies, AppLocker for Windows, and SELinux or AppArmor for Linux. |
| ICS | T0820 | Exploitation for Evasion | Make it difficult for adversaries to advance their operation through exploitation of undiscovered or unpatched vulnerabilities by using sandboxing. Other types of virtualization and application microsegmentation may also mitigate the impact of some types of exploitation. Risks of additional exploits and weaknesses in these systems may still exist. [1] |
| ICS | T0890 | Exploitation for Privilege Escalation | Make it difficult for adversaries to advance their operation through exploitation of undiscovered or unpatched vulnerabilities by using sandboxing. Other types of virtualization and application microsegmentation may also mitigate the impact of some types of exploitation. Risks of additional exploits and weaknesses in these systems may still exist. [1] |
| ICS | T0866 | Exploitation of Remote Services | Make it difficult for adversaries to advance their operation through exploitation of undiscovered or unpatched vulnerabilities by using sandboxing. Other types of virtualization and application microsegmentation may also mitigate the impact of some types of exploitation. Risks of additional exploits and weaknesses in these systems may still exist. [1] |

| Domain | ID | Name | Use |
| --- | --- | --- | --- |
| ICS | T0853 | Scripting | Consider the use of application isolation and sandboxing to restrict specific operating system interactions such as access through user accounts, services, system calls, registry, and network access. This may be even more useful in cases where the source of the executed script is unknown. |

---

Source: https://attack.mitre.org/mitigations/M0948