

Exploitation for Defense Evasion Mitigation, Mitigation T1211 - Enterprise

Archived: 2026-04-05 13:22:00 UTC

Update software regularly by employing patch management for internal enterprise endpoints and servers. Develop a robust cyber threat intelligence capability to determine what types and levels of threat may use software exploits and 0-days against a particular organization. Make it difficult for adversaries to advance their operation through exploitation of undiscovered or unpatched vulnerabilities by using sandboxing, if available. Other types of virtualization and application microsegmentation may also mitigate the impact of some types of exploitation. The risks of additional exploits and weaknesses in implementation may still exist.

Source: <https://attack.mitre.org/mitigations/T1211>