Detecting Downgrade Attacks, Detection Strategy DET0350

Archived: 2026-04-05 14:24:55 UTC

AN0995

Detection of processes launching downgraded PowerShell versions (e.g., v2) or other legacy binaries that lack logging or security features. Correlates command-line arguments, process metadata, and version fields. Monitors registry changes to Defender or HVCI keys that could indicate intentional downgrades.

Log Sources

Mutable Elements

Field	Description
AllowedInterpreterVersions	Defines which versions of interpreters like PowerShell are permitted in the environment.
RegistryDefenderKeys	Specific registry paths for monitoring Defender/HVCI configurations that may vary by Windows version.

AN0996

Monitors execution of older or legacy interpreters (e.g., python2, bash with restricted history logging), downgrade of TLS/SSL configurations, or forced fallback to unencrypted protocols. Detects suspicious reconfiguration of kernel modules or boot loaders to reduce integrity controls.

Log Sources

Data Component	Name	Channel
Command Execution (DC0064)	auditd:SYSCALL	execve: Execution of downgraded interpreters such as python2 or forced fallback commands
Process Metadata (DC0034)	linux:syslog	Kernel or daemon warnings of downgraded TLS or cryptographic settings

Mutable Elements

Field	Description
AllowedCryptoProtocols	List of TLS/SSL versions approved for use; alerts triggered if older protocols (e.g., TLS 1.0) are used.

AN0997

Detection of execution of legacy scripting runtimes (e.g., older versions of Python, Bash, or PowerShell Core) lacking auditing. Monitoring for changes to EFI or system boot files indicative of downgrade-based persistence or bypass of integrity features.

Log Sources

Mutable Elements

Field	Description
ApprovedInterpreterVersions	Defines the minimal version of interpreters expected; older versions flagged as downgrade attempts.
