Software Deployment Tools, Technique T1072 - Enterprise

Archived: 2026-04-05 18:01:36 UTC

Adversaries may gain access to and use centralized software suites installed within an enterprise to execute commands and move laterally through the network. Configuration management and software deployment applications may be used in an enterprise network or cloud environment for routine administration purposes. These systems may also be integrated into CI/CD pipelines. Examples of such solutions include: SCCM, HBSS, Altiris, AWS Systems Manager, Microsoft Intune, Azure Arc, and GCP Deployment Manager.

Access to network-wide or enterprise-wide endpoint management software may enable an adversary to achieve remote code execution on all connected systems. The access may be used to laterally move to other systems, gather information, or cause a specific effect, such as wiping the hard drives on all endpoints.

SaaS-based configuration management services may allow for broad Cloud Administration Command on cloud-hosted instances, as well as the execution of arbitrary commands on on-premises endpoints. For example, Microsoft Configuration Manager allows Global or Intune Administrators to run scripts as SYSTEM on on-premises devices joined to Entra ID.[1] Such services may also utilize Web Protocols to communicate back to adversary owned infrastructure.[2]

Network infrastructure devices may also have configuration management tools that can be similarly abused by adversaries.[3]

The permissions required for this action vary by system configuration; local credentials may be sufficient with direct access to the third-party system, or specific domain credentials may be required. However, the system may require an administrative account to log in or to access specific functionality.

Source: https://attack.mitre.org/techniques/T1072