Internet Accessible Device, Technique T0883 - ICS

Archived: 2026-04-05 14:27:02 UTC

Adversaries may gain access into industrial environments through systems exposed directly to the internet for remote access rather than through External Remote Services. Internet Accessible Devices are exposed to the internet unintentionally or intentionally without adequate protections. This may allow for adversaries to move directly into the control system network. Access onto these devices is accomplished without the use of exploits, these would be represented within the Exploit Public-Facing Application technique.

Adversaries may leverage built in functions for remote access which may not be protected or utilize minimal legacy protections that may be targeted. [1] These services may be discoverable through the use of online scanning tools.

In the case of the Bowman dam incident, adversaries leveraged access to the dam control network through a cellular modem. Access to the device was protected by password authentication, although the application was vulnerable to brute forcing. [1] [2] [3]

In Trend Micros manufacturing deception operations adversaries were detected leveraging direct internet access to an ICS environment through the exposure of operational protocols such as Siemens S7, Omron FINS, and EtherNet/IP, in addition to misconfigured VNC access. [4]

Source: https://attack.mitre.org/techniques/T0883