Department for Levelling Up,
Housing & Communities

Device & MS-365 Hardening

Workshop

V 1.0

LOCAL DIGITAL Cyber

Objective

The purpose of this workshop is to highlight the benefits of hardening and secure configuration of Local Authority information systems, and signpost useful resources to assist you.

Make attackers see your systems like:

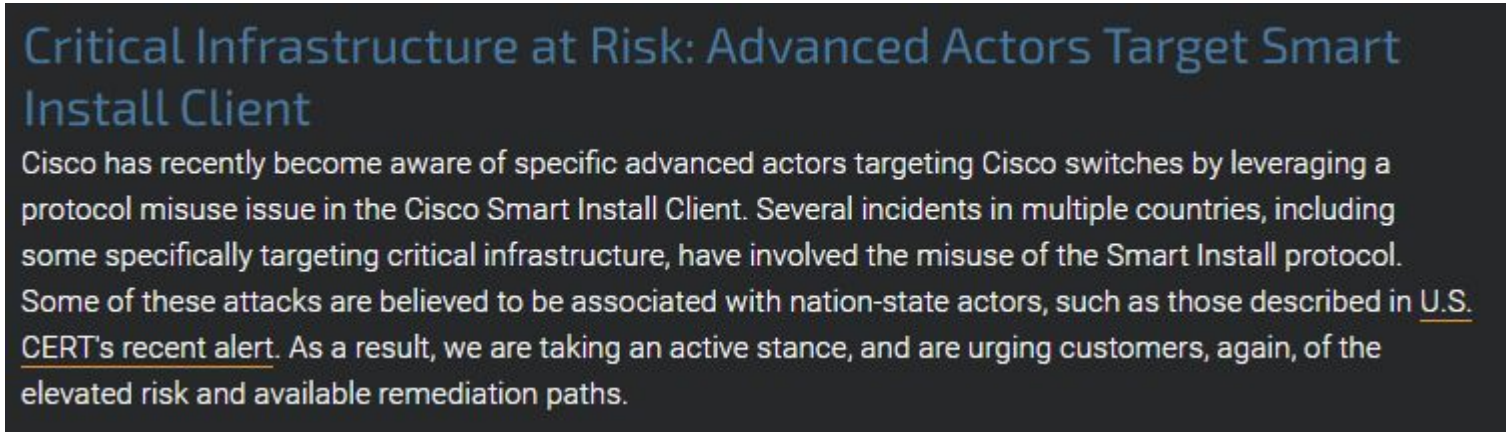
THIS

NOT THIS!

Why it's important?

According to Cisco Talos, more than 168,000 devices found on Shodan have this vulnerability.

- Blocking Initial Access Attempts:



Critical Infrastructure at Risk: Advanced Actors Target Smart Install Client

Cisco has recently become aware of specific advanced actors targeting Cisco switches by leveraging a protocol misuse issue in the Cisco Smart Install Client. Several incidents in multiple countries, including some specifically targeting critical infrastructure, have involved the misuse of the Smart Install protocol. Some of these attacks are believed to be associated with nation-state actors, such as those described in U.S. CERT's recent alert. As a result, we are taking an active stance, and are urging customers, again, of the elevated risk and available remediation paths.

According to Cisco, "The Cisco Smart Install protocol can be abused to modify the Trivial File Transfer Protocol (TFTP) server setting, exfiltrate configuration files via TFTP, modify the configuration file, replace the IOS image, and set up accounts, allowing for the execution of IOS commands.

LOCAL DIGITAL Cyber

Why It's Important?

- Block Attacker movement after initial compromise, e.g:
  - Compromised host lets attacker steal/dump/extract & reuse credentials
  - Insecure Task Scheduling allows attacker privilege escalation/persistence
  - Attacker's network foothold allows MITM / credential relaying/interception attacks

LOCAL DIGITAL Cyber

SIGN IN

The Register

Jul 2021

You, too, can be a Windows domain controller and do whatever you like, with this one weird WONTFIX trick

The end result is an authentication certificate that grants the attacker domain-controller-level access to services, allowing them to commandeer the entire domain.

- "PetitPotam takes advantage of servers," said Microsoft, "*where the Active Directory Certificate Services (AD CS) is not configured with protections for NTLM Relay Attacks.*"

LOCAL DIGITAL Cyber

Principles

Default Configuration = Insecure Configuration ?

- Each operating system/device should have a defined & documented configuration hardening baseline
- Badly written software can introduce insecure configurations
- Hardening should be regularly tested and any identified security issues resolved upon discovery & base image updated

LOCAL DIGITAL Cyber

Servers

- The Centre for Internet Security (CIS) publishes internationally recognised security benchmark configurations, and these are widely used by organisations as the basis for their security baselines. https://www.cisecurity.org/cis-benchmarks/

- Most CIS Benchmarks include multiple configuration profiles

  - The Level 1 profile is considered a base recommendation that can be implemented fairly promptly and is designed to not have an extensive performance impact.

  - The Level 2 profile is considered to be “defence in depth” and is intended for environments where security is paramount.

LOCAL DIGITAL Cyber

Linux Servers

- Over Permissive Home directory permissions e.g. 755
- setgid and setuid binaries- only logged by benchmark
- World readable and writable files/folders
- Weak services or configurations
- Insecure file shares

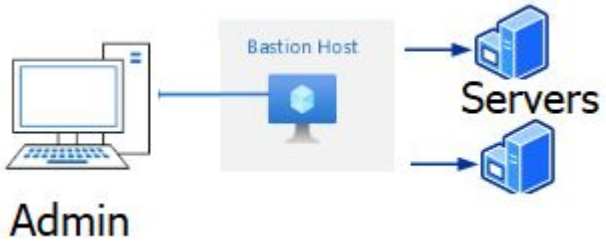
LOCAL DIGITAL Cyber

Workstations

- NCSC EUD Guidance.
  - Recommended Settings- not a Benchmark
  - Expects organisations to tailor implementation to organisation
  - Recommends a Mobile Device Management service to configure, monitor and enforce technical controls on your Windows devices + Windows Autopilot & Zero Touch Enrollment

LOCAL DIGITAL Cyber

What about Jump Hosts?



- Apply Server plus appropriate controls from the Workstation EUD guidance, e.g. AppLocker.

LOCAL DIGITAL Cyber

Network Devices

- CIS Benchmarks!!! https://www.cisco.com/c/en/us/support/docs/ip/access-lists/13608-21.html
  - Disable unused services
  - Use secure protocols
  - Management Plane protection
  - SNMP Version + Strings+ ACLs

LOCAL DIGITAL Cyber

Good practices:

- For Deployment Purposes, it is considered good practice to have a template machines for each OS and role ready, configured to your security baseline and for them to be regularly updated with the latest patches and service packs, along with any findings from your regular ITHC (IT Health Checks) and any guidance from the NCSC.
- If you use Microsoft OS ISO's, move to newer builds as Microsoft make them available.
- Disable unneeded services
- Remove unneeded Windows/Linux components
- Update builds in response to IT Health Check Findings
- Include TLS Configurations in your server builds

LOCAL DIGITAL Cyber

Microsoft/Office 365

- Not straightforward
  - Organisations use it in different ways
- Not just behind the scenes Technical Hardening
  - Some features e.g. DLP, Sensitivity Labelling require business cooperation/decisions
  - Requires correct user behaviour

LOCAL DIGITAL Cyber

NCSC/Microsoft Guidance

Good Controls	Better Controls	Best Controls
Highest Residual Risk	Lower Residual Risk	Lowest Residual Risk
M365 E3	M365 E3 + SCP or M365 E3 + E5 Security	M365 E5 or M365 E3 + E5 Security & E5 Compliance
• Enable audit logging • Enable mailbox auditing • Use Secure Score • Implement Cloud authentication • Enable MFA • Implement Conditional Access • Control access to managed devices • Block legacy authentication • Do not expire passwords • Disable accounts not used in last 30 days • Use dedicated accounts to perform Administrative Tasks • Configure Microsoft 365 Global Administrator role members • Use non-global admin accounts to perform O365 administrative tasks • Configure break glass accounts in Azure AD • Enforce MFA for all Global Admins • Enable Client Rules Forwarding Block • Do not allow anonymous calendar sharing • Configure Transport rule for ransomware • Configure anti-malware protection in your tenant • Secure external mail flow • Microsoft Teams External Access (Federation) • Microsoft Teams Guest Access • Allow SharePoint users to invite and share with new and Existing Guests • Configure data loss prevention (DLP) • Enable Office 365 Cloud App Security • Application Consent for Data Access	• Azure AD Identity Protection • Monitor user accounts for suspicious activity • Azure AD Privileged Identity Management • Schedule access reviews for privileged roles • Azure AD Entitlement Management • Configure Office 365 Advanced Threat Protection Safe Attachments feature • Configure Office 365 Advanced Threat Protection Safe Links feature • Azure Information protection - Labelling/Visible marking • Perform a simulated Attack campaign • Connect Microsoft Defender for Office to Azure Sentinel	• Enable Customer Lockbox to control Microsoft's access to organisational data. • Insider risk management • Endpoint Data Loss Protection • Extend data loss prevention to Teams chat and channel messages • Protect against data loss from cloud apps using Microsoft Cloud App Security • Restrict access to content by using sensitivity labels

Technical Guide, Office 365 UK Blueprint - Secure Configuration Alignment, Version 2,

LOCAL DIGITAL Cyber

Microsoft 365 Collaboration Blueprint for UK Government

This document contains Microsoft 365 configuration guidance developed by the Central Digital and Data Office and Microsoft. The guidance was developed to allow easier and more consistent collaboration between government organisations using Microsoft 365 services.

The configuration forms a baseline set of security and collaboration standards plus optional settings where appropriate that aim to allow HMG organisations to collaborate with a common level of trust.

LOCAL DIGITAL Cyber

The Office 365 UK Blueprint - Secure Configuration Alignment was produced by Microsoft and the NCSC and updated in April 2021. It should be implemented as a secure foundation on which to adopt the *Collaboration Blueprint*.

5.2.8 Turn on Mark new files as sensitive by default

When new files are added to SharePoint or OneDrive in Microsoft 365, it takes a while for them to be crawled and indexed. It takes additional time for the DLP policy to scan the content and apply rules to help protect sensitive content. If external sharing is turned on, sensitive content could be shared and accessed by guests before the Office DLP rule finishes processing.

Sharing Policies & Settings

The Technical Guide recommends that open external sharing is enabled. This is based on a fundamental assumption that organisations have already implemented appropriate sharing and governance policies to guide end users when sharing information outside of the organisation. Given the emphasis on these policies it would be prudent for policymakers to review the availability and awareness of such guidance. Providing the capability to share with external

LOCAL DIGITAL Cyber

Guide refers back to MS guidance..

- Setting up multi-factor authentication for guests.
- Setting up a terms of use for guests.
- Setting up quarterly guest access reviews to periodically validate whether guests continue to need permissions to teams and sites.
- Restricting guests to web-only access for unmanaged devices.
- Configuring a session timeout policy to ensure guests authenticate daily.
- Creating a sensitive information type for a highly sensitive project.
- Automatically assigning a sensitivity label to documents that contain a sensitive information type.
- Automatically removing guest access from files with a sensitivity label.

LOCAL DIGITAL Cyber

Office 365 UK Blueprint – BYOD Access Patterns

What to do next:

- Review your hardening and Baseline image generation and management activities
  - Improve where needed
- Review your use of MS 365 against the baseline guidance
  - Any areas to improve on, is business engagement needed to get their input to features?
  - Is it in a good place to consider the collab Guidance
- Review the BYOD guidance against your uses
  - Does it suggest opportunities to improve user experience or security
- Review the Collaboration Guidance
  - Discuss with the business their view on the strategy

LOCAL DIGITAL Cyber

Links

- https://cloudblogs.microsoft.com/industry-blog/en-gb/government/2021/04/14/updated-office-365-security-and-compliance-guidance-for-the-uk-public-sector/

- https://cloudblogs.microsoft.com/industry-blog/en-gb/government/2022/06/23/cross-government-collaboration-blueprint/

LOCAL DIGITAL Cyber

Staying in touch

Follow our progress

- Read our fortnightly sprint notes on Medium
- Follow LDCU on Twitter (@LDgovUK)
- Subscribe to our Cyber newsletter for progress updates and news relevant to those working in and around local government cyber security
- We'll also be sharing regular updates on the DLUHC Digital blog

Have your say

We welcome further collaboration and input, so if you would like to share with us any strong evidence to support our research please email cybersupport@localdigital.gov.uk.

LOCAL DIGITAL Cyber

Department for Levelling Up,
Housing & Communities

Thank you

We welcome feedback on our cyber support service

@LDgovUK

www.localdigital.gov.uk

#LocalDigital #FixThePlumbing

LOCAL DIGITAL Cyber