System Administrator Security Preventative Measures Landing Page

System Administrator Security Preventative Measures Landing Page

On this page:

Overview

IT providers should consider using management tools (for endpoints, mobile devices, and servers) to centralize the deployment and installation of security software and controls(Jamf Pro for Mac and MECM / SCCM for Windows) across the environment.

To further protect their systems, providers should stay informed of available patches for operating systems to ensure you're up to date with the latest security fixes. Performing regular vulnerability scans will help identify critical OS and third party software application vulnerabilities that may be installed on your systems. This information should be incorporated into a regular patch and vulnerability management cycle.

You may also be interested in joining the IT Partners or Security FYI lists to stay up to date on the latest IT and information security news.

- For more information on how to classify and secure your data, see Information Protection @ MIT.

Endpoint Management Tools

- IS&T's Endpoint Management Services

System Center Configuration Manager (SCCM)

- MECM / SCCM Service
- MECM / SCCM Software Center
- MECM / SCCM Landing Page

Jamf Pro

- Jamf Pro Service
- Jamf Pro Self Service
- Jamf Pro Landing Page

Mac Imaging

- macOS Imaging via Apple Device Enrollment Program

Windows Imaging

- Windows Imaging Service via IS&T Lite Touch

Vulnerability Scans

Vulnerabilities are weaknesses or flaws in hardware or software that can be exploited by malicious users to steal information, gain unauthorized access/privileges, manipulate system activity or cause damage to assets. Depending on the damage potential, vulnerabilities are rated on a scale of low to critical with several online databases that keep track of all vulnerabilities discovered and reported, to include https://nvd.nist.gov/, and corrective actions users should take to fix weaknesses. It is a best practice to prioritize the remediation of critical and high rated vulnerabilities.

How To

1. Identify the hosts/ip addresses within your area of responsibility by completing an inventory. See the KB here.
2. Search for the vulnerability at kb.cert.org and implement the solution recommended.
   Result: Subsequent vulnerabilities scans should show fewer vulnerabilities as they are remediated.

More Information

- Center for Internet Security for Continuous Vulnerability Management
- SANS Whitepaper on Implementing a Vulnerability Management Process
- National Vulnerability Database
- Contact the security team for more information

Have Questions or Still Need Help?

- For endpoint management assistance: euc-help@mit.edu
- For network vulnerability scan assitance: your local IT provider or security@mit.edu