US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM

Technical Information Paper-TIP-11-075-01
System Integrity Best Practices

The two key components of system integrity are **software authenticity** and **the assurance of user identity**. US-CERT recommends that organizations routinely evaluate how to integrate the following best practices into their current environments to achieve these objectives.

- Enable strong logging.
    - Enable logging for all centralized authentication services and collect the IP address of the system accessing the service, the username, the resource accessed, and whether the attempt was successful or not.
    - Limit the number of authentication attempts and lockout the user if the limit is reached. Security professionals should conduct a manual review before unlocking the account and prohibit automatic unlocks after a specified time period.
    - Conduct near real-time log review for failed attempts per user and per unit of time independent of successful logins; abnormal successful logins; and lockouts. Correlate this data to identify anomalous activity.
- Limit remote access.
    - Restrict access by IP address wherever possible.
    - Limit concurrent logins to one per user.
- Apply additional defense-in-depth techniques.
    - Maximize complexity of passwords, passphrases, and personal identification numbers (PINs) whenever possible.
    - Enable defenses against key logging such as forced frequent credential changing and updated anti-virus (AV) signatures.
- Validate software.
    - Require validation of vendor-provided hash values or digital signatures prior of installation. If information is not customarily provided, request validation guidance from the vendor.
    - Exercise additional caution when receiving unsolicited or unexpected software media.
    - Establish installation baseline (e.g., file names, versions, hash values) and periodically revalidate this information.
    - Enable revocation checking to include Online Certificate Status Protocol (OCSP) and Certificate Revocation List (CRL) checking.

Contact US-CERT

For any questions related to this paper, please contact US-CERT at:
E-mail: soc@us-cert.gov
Voice: 1-888-282-0870
Incident Reporting Form: https://forms.us-cert.gov/report/

Document FAQ

What is a TIP? A Technical Information Paper (TIP) is issued for a topic that is more informational in nature, describing an analysis technique, case study, or general cybersecurity issue. Depending on the topic, this product may be published to the public website.

If this document is labeled as UNCLASSIFIED, can I distribute it to other people? Yes, this document is intended for broad distribution to individuals and organizations interested in increasing their overall cybersecurity posture.

Can I edit this document to include additional information? This document is not to be edited, changed or modified in any way by recipients. All comments or questions related to this document should be directed to the US-CERT Security Operations Center at 1-888-282-0870 or soc@us-cert.gov.