US-CERT

UNITED STATES COMPUTER EMERGENCY READINESS TEAM

US-CERT Advisory-11-076-01: Increased Threats to Authentication Services

March 17, 2011

OVERVIEW

Authentication establishes the trusted relationship between the user and a system or service and validates their identities to each other. Organizations rely on authentication services to protect important data by limiting access to trusted users. Malicious actors are increasingly interested in exploiting authentication services because organizations rely on them to ensure system integrity and limit access to sensitive data by trusted users. US-CERT is providing this advisory to warn organizations about increased threats and interest in authentication services and provide recommended best practices to strengthen system integrity.

RECOMMENDATIONS

US-CERT recommends organizations evaluate the implementation of the following best practices to verify user identity and software authenticity:

- 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 advisory, 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/