Software features and inherent risks: NIST's guide to rating software vulnerabilities from misuse

July 26 2012

A new guide from the National Institute of Standards and Technology (NIST) describes a "scoring system" that computer security managers can use to assess the severity of security risks arising from software features that, while beneficial to accomplishing a task, are at least partially designed under an assumption that users are operating these features as intended.

NIST's Common Misuse Scoring System (CMSS) provides a systematic way for organizations to determine the severity of software feature misuse—dangerous or illicit email practices, for example—so that the organization can determine how to handle the problem.

"No system is 100 percent secure: every system has vulnerabilities," according to the report. While attention often focuses on software flaws, for example system crashes, software features also introduce vulnerabilities because intentional or accidental misuses of software features have the potential to leak sensitive information, corrupt data, or reduce system availability.

NIST categorizes software vulnerabilities in three general categories. Software flaws—coding errors that allow security breaches—are an obvious problem. Configuration vulnerabilities come from setting the software up improperly—allowing a program access to data it shouldn't see, for instance. But software feature misuse is more subtle. With

feature misuse, savvy attackers violate the trust assumptions that are inherent in software features to subvert a system's security.

For example, malicious users may undermine the security of email software. "Two common problems are social engineering and insider threats," explained Karen Scarfone, one of the publication's authors. When users open up a bad email attachment or link, the hackers who sent the email can access the organization's computer network to steal valuable information or bring it down. Malicious users can use email attachments to send out valuable company data or documents to outsiders. Both problems can be very expensive, costing a company money, exposing valuable data and hurting the company's reputation.

The CMSS specification allows the risk assessment manager to determine a vulnerability's potential impact on the network and then take remediation steps to secure the system.

The CMSS specification is designed to work with existing scoring systems developed by NIST to categorize software flaw vulnerabilities* and security configuration issues.**

More information: The new guide, The Common Misuse Scoring System (CMSS): Metrics for Software Feature Misuse Vulnerabilities, (NISTIR 7864) is available at csrc.nist.gov/publications/nis … 7864/nistir-7864.pdf

* The Common Vulnerability Scoring System (CVSS) and Its Applicability to Federal Agency Systems (NISTIR 7435) is available at csrc.nist.gov/publications/PubsNISTIRs.html

** The Common Configuration Scoring System (CCSS): Metrics for Software Security Configuration Vulnerabilities (NISTIR 7502) is available at csrc.nist.gov/publications/PubsNISTIRs.html

Provided by National Institute of Standards and Technology