A publication providing information on infrastructure protection issues, with emphasis on computer and network security matters.

Issue 02-02
May 15, 2002

Editors: Linda Garrison
          Martin Grand

- Information Technology Information Sharing and Analysis Center
- Buffer Overflows: Well-known Problems Persists in the Face of Increased Awareness
- Security Implications of Software Quality: Software Patch Management Workloads are a Part of Larger Problems
- Advance Fee Fraud: Infrastructure Providers Should Not Be Deceived

We welcome your comments and suggestions for improving this product. For more information, or to be added to the distribution list, please contact the NIPC Watch at nipc.watch@fbi.gov or call (202) 323-3204. This issue has an overall classification of "Unclassified." This publication may be disseminated further without express permission.
Information Technology Information Sharing and Analysis Center

This article continues our series of overviews of critical infrastructure industry initiatives established in response to Presidential Decisions Directive 63 (PDD-63).

The Information Technology Information Sharing and Analysis Center (IT-ISAC) is a forum for sharing information about network vulnerabilities and related threat and countermeasure information. The IT-ISAC is a non-profit corporation with approximately twenty member corporations that:

- Report and exchange information among industry members regarding electronic incidents
- Collaborate on newly-discovered software vulnerabilities and countermeasure development
- Promote strategies to protect against hostile action
- Assist in maintaining continuity of operations and rapid recovery

In the twelve months following its inception, the IT-ISAC has made available to the public a number of analyses on software vulnerabilities and recommendations to improve the overall network security environments.

The IT-ISAC provides a means for critical infrastructure sector members whose business emphasis is, or depends on, Information Technology to freely exchange information regarding security incidents without revealing information that may otherwise be subject to Freedom of Information act and Open Record laws. The ability to maintain this privacy is important to any corporation looking to guard its proprietary information while collaborating with like entities in defending against an attack.

In January 2002, the IT-ISAC and the NIPC signed an information exchange Memorandum of Understanding (MOU). The MOU specifies, among other things, that:

“The IT-ISAC will report on a voluntary basis to provide the NIPC with … information on unscheduled service outages, degraded operations and serious threats to information systems and networks, provided they meet mutually established reporting criteria and thresholds … Likewise, the NIPC will provide the IT-ISAC with the following types of information, at its discretion, concerning the IT-infrastructure: unscheduled service outages, degraded operations, Distributed Denial of Service Attacks, virus alerts, network scanning, or spoofing of networks.”

For more information on the IT-ISAC, please visit their web site at https://www.it-isac.org, send an email to operations@it-isac.org, or phone (404) 236-2880.
Buffer Overflows: Well-known Problem Persists in the Face of Increased Awareness

Despite being one of the oldest known computer security problems, buffer overflows continue to be the most prevalent type of attack on the Internet. In 2001, 19 CERT advisories, out of a total of 37, warned of vulnerabilities resulting from overflows. Most recently, warnings concerning the serious defects in SNMP included inherent vulnerabilities to buffer overflow attacks. This flaw is frequently targeted because of the opportunity it offers for remote attackers to gain root access of a victim’s computer.

Buffer Overflows

A buffer overflow results when an attempt is made to place more data in a temporary storage area, known as a buffer, than it was designed to hold. A basic example consists of a program requiring some type of input, such as a username. A programmer must reserve a spot in memory to hold this data, entering more data into the buffer than a programmer has allotted can cause it to overflow. When the data exceeds the bounds of the buffer, it can overflow into other areas of memory, which may allow an attacker to inject and run malicious code.

While this type of attack has been around for quite some time, the frequency increased greatly in the 1990’s, due largely to several infamous papers published on the Internet detailing the ABC’s of exploiting this vulnerability. In addition to online tutorials, the availability of automated tools designed to exploit buffer overflows caused a significant escalation of this type of attack. This had the effect of enabling novices, who previously may have lacked the required skills to write their own exploits.

Prevention

Buffer overflows are the result of poor programming practices, primarily in the C and C++ programming languages. Taking steps to ensure size limits are not exceeded, known as bounds checking, and avoiding unsafe string operations can mitigate this issue.

There are, however, many programs containing legacy code/libraries, which are still in use. Reviewing these programs can be daunting, as some programs are based on many hundreds of thousands of lines of code. Even after extensive review, problems can still surface. Steps to alleviate problems with buffer overflows include the following:

- When possible, avoid running services with root or administrative privileges. In that when when an attacker runs exploit code, they inherit the privileges that the service is running under. Running at a lower privilege level can limit the attack.
- Coding in safer languages, when appropriate, can reduce overflows.
- It is critical that system administrators keep track of newly discovered vulnerabilities and patch systems immediately (the NIPC’s CyberNotes can help when planning priorities).
- The bottom line – Emphasize avoiding buffer overflows during the software design and testing phases as a software quality objective to reduce the prevalence of buffer overflow vulnerabilities.
Security Implications of Software Quality:
Software Patch Management Workloads Are A Part of Larger Problems

Protecting against Known Software Vulnerabilities Account for the Majority of time Dedicated by System Administrators. Software patch deployments to address security issues are widely regarded as a major component of system administrators’ workloads. In November 2001, Activis, a UK security company, reported research illustrating the contribution of patch deployments to system administrators’ workloads. Activis found that a relatively small network of mixed vendor products with only eight firewalls and nine servers would have required 1,315 vendor software updates, or five per day, during a nine-month period in 2001.

Software User and Computer Security Community Views on Quality and Security. Many in both the software user community and computer security community believe that constant releases of vendor software patches result from vulnerabilities and problems that should have been detected and corrected before vendor software packages are released. Additionally, it is viewed that rushing software to market, results in quality and security not being “designed in.” Users see quality and security being addressed later, often after the software packages have been widely deployed to customers.

Software Vendors’ Views on Quality and Security. Software vendors do not intentionally produce defective code. They are concerned for both the reputation of their brand names as well as for customer impacts that software quality problems cause. Vendors also note that some problems experienced by users are not solely based with issues that vendors can control. User demand has contributed to “feature creep” resulting in software packages with many more lines of code and increasingly complex security requirements. Customization of vendor software by user organizations often introduces new problems. Additionally, some technical professionals note that system administrator training problems, insufficient management emphasis on security, and poor security practices and policies contribute to security concerns of which software quality issues are only one factor.

Critical Infrastructure and Enterprise Network Implications: Progress improving software quality and security in networks and infrastructures can only result if all parties address the issues contributing to the problems. Vendors must continue initiatives to improve software quality, particularly in areas with security implications. Software user organizations, including government, must improve the management and practice of security. Key references for user organizations include:

- **CERT® Security Improvement Modules** provide an overview of managing the functions of security at [http://www.cert.org/securityimprovement/#modules](http://www.cert.org/securityimprovement/#modules).
- **The SANS/FBI Twenty Most Critical Internet Security Vulnerabilities (Updated), The Experts’ Consensus, Version 2.501, November 15, 2001** provides a prioritized approach to addressing the most dangerous security issues involved in the majority of successful computer system attacks at [http://www.sans.org/top20.htm](http://www.sans.org/top20.htm).
Advance Fee Fraud: Infrastructure Providers Should Not Be Deceived

The spread of the Internet is removing barriers to communication of all types, including those with criminal intent. Fraudulent solicitations targeting individuals and companies are increasingly being disseminated via e-mail.

Advance Fee Fraud. One well-known type of scheme generally known as advance fee fraud involves an attempt to trick a victim into making up-front payments with the promise that his investment will lead to a large payoff in the future. These scams typically begin with a letter or fax—or, more recently, an e-mail—overtly sent by a government official or businessperson in a foreign country. The letter relates a cover story that the writer is looking for a trustworthy person or company in the U.S. to help recover funds related to “an over-invoiced government contract” or “contract overpayments” or other questionable source. The victim is offered a large commission in order to assist in an international bank transfer and is requested to provide company letterhead and/or financial details such as bank account information in order to facilitate the transaction. Victims may also be asked to forward funds to cover various “bank fees” or “transfer taxes” or other up-front expenditures.

There are many variations of this type of fraud. Some scams offer crude oil allocations at below market rate, if the victim is only able to pre-pay certain licensing fees or duties. Others solicitations relate a bogus story of needing a front company to facilitate an oil or telecommunications contract for a group of civil servants. The deception may be remarkably elaborate, possibly including invitations abroad or the planting of bogus articles in foreign media to provide a pretext for the deception. There are estimates that damages caused by advance fee fraud amount to hundreds of millions of dollars annually.

The Infrastructure Connection. Many advance fee solicitations ostensibly originate from infrastructure-related entities: a bank; a national petroleum corporation, electric power authority, or other entity in the energy industry; a national telecommunications company; or a government financial ministry or regulatory body responsible for overseeing mineral resources. Some also purport to deal with the provision of infrastructure-related services. There is, however, no legitimate infrastructure connection in these solicitations; law enforcement data indicate that fraud artists specializing in advance fee schemes utilize international business directories, trade and business journals, media advertisements, and the Internet to locate prospective victims.

Infrastructure providers should not confuse advance fee solicitations with legitimate business offers from abroad. If they receive a letter or e-mail of this type, infrastructure providers should not be deceived by any ostensible industry links mentioned in the solicitation. The U.S. Department of Commerce can assist U.S. businesses in establishing the legitimacy of international business proposals. Fraudulent business solicitations should be referred to the Financial Crimes Division of the U.S. Secret Service or to the Internet Fraud Complaint Center run by the Federal Bureau of Investigation and the National White Collar Crime Center on the Internet at <http://www.ifccfbi.gov>.