Global Information Assurance Certification Paper

Applying security patches would reduce significant vulnerabilities
William T. Ainge
March 31, 2001

Background

"The General Service Administration in February 2001 called on Industry to help define a system for agencies to stay on top of the abundance of software patches that companies issue to cover security vulnerabilities in their products. The GSA Office of Information Assurance and Critical Infrastructure Protection issued a request for information for the system, which would address an awareness problem among agencies worldwide. Many security breaches happen when attackers take advantage of vulnerabilities for which patches are available, but system administrators have not applied the patches" [1].

"The distributed denial-of-service attack that downed electronic commerce sites a year ago this month occurred primarily because patches had not been applied on systems attackers used to flood sites, according to officials. Furthermore, audits by the General Accounting Office found that the failure to apply security patches opens significant vulnerabilities in Federal systems security" [1]. GAO attributed the cause to lack of policy requirements for correcting identified deficiencies and vulnerabilities [2,3].

"The Federal Computer Incident Response Capability (FEDCIRC) stated that agencies indicated: a lack of personnel with the time and expertise to stay on top of the changes to secure an agency's connection to the world. "Many system administrators are doing the job part time, or it was handed to other duties and they are just not able to keep up with the changes" said a federal official. While IT staff members are already overwhelmed, alerts continue to roll in and old problems are not going away. According to FEDCIRC, nearly all of the recent Web site defacements have been accomplished by people penetrating holes for which patches are available" [4].

"Vendors providing patches to fix security weaknesses work with the CERT Coordination Center (CERT/CC) located at the Software Engineering Institute (SEI), a federally funded research and development center at Carnegie Mellon University in Pittsburgh, Pennsylvania. Following the Internet Worm incident, which brought 10 percent of Internet systems to a halt in November 1988, the Defense Advanced Research Projects Agency (DARPA) charged the SEI with setting up a center to coordinate communication among experts during security emergencies and to help prevent future incidents" [5].

1

2,3

4

5

"Since then, the CERT/CC has helped to establish other response teams and their incident handling practices have been adopted by more than 85 response teams around the world. To accomplish their goals, they focus their efforts on the following areas of work: survivable network management, survivable network technology, incident handling, incident and vulnerability analysis, courses and seminars. CERT/CC is also committed to increasing awareness of security issues and helping organizations improve the security of their systems. CERTCC publishes security improvement modules such as "Keep operating systems and applications software up to date" [5,7]. They disseminate information through several channels, two of these pertinent to this discussion are:

Vulnerability Analysis

"The CERT/CC has become a major reporting center for both incidents and vulnerabilities because they have an established reputation for discretion and objectivity. When they receive a vulnerability report, their vulnerability experts analyze the potential vulnerability and work with technology producers to inform them of security deficiencies in their products and to facilitate and track their response to these problems. Another source of vulnerability information comes from incident analysis. Repeated incidents of the same type often point to the existence of an vulnerability and, often, the existence of public information or automated tools for exploiting the vulnerability. The CERT/CC makes vulnerability information widely available through the Vulnerability Catalog in the CERT Knowledge base at" [5]. http://www.kb.cert.org/vuls/

Advisories – "CERT/CC advisories address Internet security problems. They offer an explanation of the problem, information that helps you determine if your site has the problem, fixes or workarounds, and vendor information. Among the criteria for developing an advisory are the urgency of the problem, potential impact of intruder exploitation, and the existence of a software patch or workaround. On the day of release, CERT/CC sends advisories to a mailing list, post them to the USENET newsgroup http://www.comp.security.announce and make them available on the CERT web site at" [5]. http://www.cert.org/advisories/

Problem

As the GAO indicated significant vulnerabilities are present when available patches are not applied. It also encompasses a new federal focus on getting agencies and industry to use the tools and patches that are available before they are needed, not after [6]. Some of the reasons for not applying patches are caused in my judgement by manual procedures, lack of controls and not automating the function. As a result, organizations are needlessly vulnerable to known attacks for which protection could have been applied.

5,7

5

5

6

Other factors can cause patches not to be applied at all or applied too late to protect against a hacker. The following is based on my experience with a large organization and how their Advisory process was not as effective in applying patches as it could be. This organization had a centralized distribution and accounting for patches with their field activities responsible for actually applying the patch. The field organizations had LAN configurations with firewalls and anywhere from 1 to 20 servers (Windows NT, Unix) with hundreds of workstations attached and WAN connectivity.

Field offices had to determine which patches were applicable

Distribution of Patches was accomplished by the headquarters Information System Security Officer (ISSO) receiving patches from a central headquarters location that received them from CERT CC. The ISSO then forwarding them via email to all field offices. The patches were not reviewed prior to sending them to offices to determine if they were applicable to a given field office because: office configuration data was not current; and no automated system had been developed to review Advisories and determine what offices should receive patches.

Originally, reviews of patches for applicability was done by system administrators but they did not review them promptly which delayed the sending of Advisories. As a result, each field office ISSO and System Administrator had to review the documentation for the patch to determine if it was applicable to their systems. Many Field Administrators complained about repetitively receiving patches that were not applicable to the products they had installed. They complained that reading Advisories for patches that were not applicable took time they could have been spending on applicable patches.

All field offices had to download patches from the vendors web site

Field offices had to access the vendor specified web page to download the patch. Each field office had to select the correct patch for their configuration from the vendors Web page. This caused more work then if one central office location downloaded the patch making sure the right patches were downloaded for all the field offices by the configuration they have.

Automation is needed to manage Security Advisories

After field office system administrators completed applying the Advisory patch to the systems affected, an email was sent to notify headquarters security personnel. Each email was reviewed by security to determine if they stated the patch was applied or it was not applicable to their configuration. Manual logs had to be kept to record reporting statistics such as number of servers, work stations, routers, firewalls, downtime, bad files, etc. All of this data had to be manually

summarized by security for reporting purposes including the number of offices who applied the patch and those that didn't by the deadline set for the Advisories.

This required security personnel to devote hours on a daily basis to the collection of data from emails regarding patches. Additionally, field offices created their own files for keeping track of their Advisories since no Advisory database existed. If an Advisory database existed it would have Advisory records created by the headquarters ISSO and maintained by the field office ISSO.

The database would be Web enabled so the field could update their records with completion date, number systems affected, etc. The database would also provide a means for field offices and headquarters to keep track of all their Advisories progress. Management agreed with the need for a database but did not apply any resources due to other priority work.

Field offices were late in meeting Advisory deadlines 60 % of the time

Typically, the field offices were given anywhere between one to two months to meet the requirements in an Advisory. Of course for critical Advisories and Tasking they were only given one day or a few days. Some of the same field offices were late over and over again with Advisories being completed sometimes months later if ever. However, they were not held accountable for why they were so late. No system or procedure existed for the regular review of which offices were late applying Advisories. Field offices indicated that the system administrators lacked the time especially on patches that had to be applied to every workstation in the office. The headquarters security department themselves short of time accepted that little could be done to improve response time. Offices were so behind on Advisories that headquarters security did not run on a regular basis scanning software that highlights missing patches.

Lack of Software tools prevented patches being applied centrally

As previously stated the headquarters lacked software tools to apply patches to firewall, server and workstations through one central server. However, the headquarters did obtain such software and servers for the entire organization to implement System Management Software (SMS) but implementation has been very slow. One or two field offices have SMS implemented and are using it to apply patches. Implementation may not achieve true centralization of applying changes to field offices. Headquarters wanted to first send to the field office SMS server the changes and the filed office will use that server to make the changes. This could put us right back to where we started with delays and perhaps some patches not even being applied. For SMS or other software to be successful in patch processing across a large network organization it has to allow for application from one central server. Using this software centrally would eliminate many of the reporting problems except where the field offices still have to perform the Advisory.

Recommendations:

My observations of problems with processing of Advisory patches were based on a large organization with a Headquarters supporting many remote locations. However, these problems may be occurring in small to medium sized organizations so they might benefit from reviewing the problem areas I mentioned. Based on the existing problems I would recommend the following:

1. Implement software capable of applying patches from the corporate location to all field offices firewalls servers, workstations. This will prevent many of the delays caused by offices not applying patches on time. This will reduce the amount of Advisory management that will need to be performed. If the software can't be used to update all field servers and workstations, it still should be installed on the field servers so they can apply their workstation changes.

2. For patches that can't be done by corporate the Security and System Administrators determine by reviewing accurate configuration data for offices which patches are applicable. Software to automatically do this would be best but if it can't be obtained it still needs to be performed manually. Send only those patches that are applicable to offices.

3. For patches that still have to be implemented by field offices provide a central file where they can obtain the downloaded patches with explanation of which patch to use.

4. Implement software where a central web enable database can be used to track the issuance and receipt of Advisories sent to field office. Provide for updating of their database Advisory records from the field. Also reporting software to be used to report Advisory completion statistics and tracking of late responses.

5. Require that procedures be developed and used to report Advisory patches not applied on time and by what offices.

Conclusion

Adopting some or all of the recommendations should significantly improve the security posture of organizations. Time required to update patches would decrease along with increased headquarters security control over ensuring patches were made. Less system administrators would be required to apply the patches. Security personnel could spend more time on security issues rather then opening email with field office responses. Management support is needed to accomplish the recommendations. They need to be made aware that doing nothing will continue to result in patches being applied too late or not at all increasing the odds that a hacker will compromise the system.

References:

(1) Frank Diane "Industry asked to help with patches" Federal Computer Week 2/20/01 page 1 paragraph 1-4. (3/10/01) URL: http://www.fcw.com/fcw/articles/2001/0219/web-patch-02-20-01.asp

(2) Government Accounting Office – " Federal Information Security: Actions Needed to Address Widespread Weaknesses": 03/29/2000 Page 1. (3/14/01) URL: http://frwebgate.access.gpo.gov/cgi-bin/useftp.cgi?IPaddress=162.140.64.21&filename=ai00135t.txt&directory=/diskb/wais/data/gao

(3) Government Accounting Office – " Computer Attacks at DOD pose increased risks" 05/22/96 chapter 0:3.4 paragraph 2 & chapter 3:2 paragraph 3 (3/14/01) URL: http://frwebgate.access.gpo.gov/cgi-bin/useftp.cgi?IPaddress=162.140.64.88&filename=ai96084.txt&directory=/diskb/wais/data/gao

(4) Frank Diane and Thimble Paula – " Feds leave door open for hackers" Federal Computer Week 12/20/99 page 1&2. (3/24/01) URL: http://fcw.com/fcw/articles/1999/fcw-newshackers-12-20-99.asp

(5) Carnegie Mellon Software Engineering Institute – "Meet the CERT Coordination Center" (03/27/01) page 1 & 3 URL: http://www.cert.org/meet_cert/meetcertcc.html

(6) Frank Diane – "Feds to industry: You have a responsibility for security too" Federal Computer Week 02/16/00. (3/26/01) URL: http://www.fcw.com/fcw/articles/2000/0214/web-industrysecurity-02-16-00.asp

(7) Carnegie Mellon Software Engineering Institute – "Keep operating systems and applications software up to date (3/24/01) URL: http://www.cert.org/security-improvement/practices/p067.html

1

Last Updated: July 25th, 2017

Upcoming Training

SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor
SANS Phoenix-Mesa 2017	Mesa, AZ	Oct 09, 2017 - Oct 14, 2017	Live Event