



Interested in learning
more about security?

SANS Institute InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Patch DoS

With the current economic situation throughout the world (2001), recent events regarding homeland security in the United States, and the ongoing transition into a new E business era, the pressure to secure our networks and systems has resulted in some troubling trends. While we are all aware of the "ship first, patch later" methodology used in most IT projects, we are just starting to feel the ramifications of these methods as they relate to security in a 24x7x365, ecommerce environment.

Copyright SANS Institute
Author Retains Full Rights

AD

DEEPARMOR®

Patch DoS

December 12, 2001

Chad Oleary

Background

“Research carried out by Activis on upgrades required for several leading products, has shown that for a company with an infrastructure of only 8 firewalls and nine servers, the IT manager would have had to make 1,315 updates in the past nine months, year to date. This is equivalent to five updates per working day. In addition, they would be expected to manage over half a million log file entries every day.” (1)

Introduction

With the current economic situation throughout the world, recent events regarding homeland security in the United States, and the ongoing transition into a new E business era, the pressure to secure our networks and systems has resulted in some troubling trends. While we are all aware of the “ship first, patch later” methodology used in most IT projects, we are just starting to feel the ramifications of these methods as they relate to security in a 24x7x365, e-commerce environment.

Too Many Patches, Not Enough Time

From the example provided above, you can see that the situation is bad. To compound this, recent outbreaks of Code Red, Nimba, et al., have left most organizations in a situation that could be termed “Patch DoS”. Put simply, the industry is nearing a Denial of Service condition due the timing and frequency required by the patch process. The research from Activis goes even further to say that this is “jeopardizing network security.” (1)

We can look to the past of software development for some clues as to what has happened and what we can expect. What if Netscape had taken the time to “do it right?” Would we even know about them? How about this story from an IBM software engineer: "I have installed software that did not work at all. When I reluctantly printed out the readme, it said that this software requires a patch available on the Internet. I could hardly believe that a manufacturer would ship software that was completely broken and then require its users to download a patch to enable it to work." (2)

To compound the issue, clustered systems to provide High Availability usually need to have the entire cluster taken offline, upgraded, and then, hopefully, restored to service. Try doing this to your HSRP routers, firewalls pairs, redirection devices, and operating systems at your e-commerce site. You'll quickly find out that you've spent so much time patching these systems that you're now out of business.

What? These systems are not patched?

From time to time we have all run into that one application that refuses to cooperate as attempts are made to patch the underlying operating system. At this point we need to bring in the programmers and dig through the code to find the culprit so that the operating system can be patched. Now the IT manager is faced with more than a simple patch, it's now diverted virtually all the resources at her disposal. To compound the matter, patches are supposed to be "infrequent", so often policies generally do not exist and time is not allocated to allow for these efforts.

Another notion that was presented by Stephan Somogyi, of ZDNet:

"One reason why security-related updates aren't being installed is almost certainly inertia. The system isn't crashing and anyone who's spent more than a few days being a system administrator knows that good updates can go very bad indeed and wreak havoc with one's uptime. Better to leave well enough alone, some might think." (3)

While this may still be the case at some shops, I think we have all seen recent events turn even the most die-hard uptime fan turn into a patch believer. However, in the context of addressing the patch problem, Mr. Somogyi goes on to say, "Bruce Schneier argues that a standardized certification entity is a bad idea, and his arguments are reasonable. However, the FBI's dire warnings are unlikely to have any effect until there's some kind of enforcement oomph behind it." (3)

Certified to Patch

Bruce Schneier fittingly describes the founding of Underwriters Laboratories in a special to ZDNet:

"Underwriters Laboratories (UL) is an independent testing organization that rates electrical equipment, safes, and a whole lot of other things. It all

started in 1893, when William Henry Merrill was called in to find out why the Palace of Electricity at the Columbian Exposition in Chicago kept catching on fire (not the best way to tout the wonders of electricity)." (4)

The example that Mr. Schneier offers is that of a safe, "Safes, for example, are rated based on time and materials. A "TL-15" rating means that the safe is secure against a burglar limited to safecracking tools (and not torches or explosives) and 15 minutes' working time." (4).

These ratings are exactly what the Center for Internet Security is beginning to initiate for IT systems. The members of this organization are the same players that have helped bring security out of the unspoken world and into the boardroom, such as ISC² and SANS. As part of this process to rate and evaluate the security of server and network operating systems, the Center for Internet Security intends to rate these systems on a scale of 1-10. The center has released several tools in assessing the security of networked systems. They have released platform specific tools to perform a benchmark analysis of Windows 2000 and Solaris. They have also released "An Automated Scanning Tool for the SANS/FBI Top Twenty List." (5)

With tools like this in place, we can begin to bring some order to the patch process. Not only do we now have the ability to rate which patches need to be applied first, and where, but we can also show a benchmark for our progress. To help things even more, these tools can be used again and again to determine if a patch has created "new" problems that were unexpected. Also, they can help benchmark the successes or failures of many of the proposed upgrades to the patch process.

Patching the Patch Process

One of the proposals with Microsoft's recent security commitment is to integrate the patch delivery process for security related patches into Anti-Virus updates. While this has its own set of political and technical concerns, none quite so directly impact the security community as the issues regarding policy:

"Eric Chien, chief researcher at antivirus firm Symantec, said the threat is likely to be compounded by Microsoft's dot-Net strategy for online software. 'Dot-Net uses a policy-based approach to security. The transition to dot-Net is potentially a nightmare for administrators, who will need to be sure that all their policies are correct. The ability to roll out patches to these firms will not help them to set their policies correctly,'" (6)

The dot-Net strategy to approach security via policy is an excellent way to help the small and medium sized companies to begin to understand policies, and their

role in any sized networked environment. However, if these patches overwrite policies previously defined, this could be a major hindrance to acceptance of policy at any organization.

Cryptosystem design has already proven that the concept of peer review and open development works quite well. DeCSS has proven quite well that closed cryptosystems will almost certainly succumb to compromise. These peer reviews and disclosures have been key in identifying and closing security weakness on all major vendors products – whether they be closed or open source.

In reaction to recent events, Microsoft is successfully creating a closed circle for disclosure of potential vulnerabilities, rather than have them disclosed publicly. While this may help keep the “script kiddies” from getting their hands on tools to wreak havoc with the Microsoft product line, is it going to help get the vulnerabilities patched? Already, the indications are no. Recently, Jouko Pynnonen of Oy Online Solutions, Ltd. submitted a serious flaw to Microsoft in their browser:

“Oy Online Solutions Ltd's security experts have found a flaw in Microsoft Internet Explorer that allows a malicious website to spoof file extensions in the download dialog to make an executable program file look like a text, image, audio, or any other file. If the user chooses to open the file from its current location, the executable program will be run, circumventing Security Warning dialogs, and the attacker could gain control over the user's system.

VENDOR STATUS

Microsoft was contacted on November 19th. The company doesn't currently consider this is a vulnerability; they say that the trust decision should be based on the file source and not type. The origin of the file, ie. the web server's hostname can't be spoofed with this flaw. It's not known whether a patch is going to be produced. Microsoft is currently investigating the issue.” (7)

To date, @stake, Bindview, Foundstone, Guardent, Internet Security Systems, and Microsoft have announced their intention to participate in this organization. Other members are expected to join the organization in the coming weeks. The current members have proposed using the RFC process to develop future standards for security disclosures. Three characteristics are to be present in each standard developed:

“Comprehensive. They would cover virtually all aspects of a recommended security vulnerability handling process, including topics like how and where to report a security vulnerability; how long a vendor should

take to investigate the report; and the format and content of a security advisory. They would discuss the obligations of both vendors and researchers.

Collaborative. The standards would provide a framework for a cooperative, collegial relationship between vendors and security researchers that helps all of us deliver on our mutual goal of protecting computer users.

Broadly accepted. Because the standards would be developed as part of the open RFC process, all interested parties would have an opportunity to review drafts and provide feedback. It is our hope that the standards will represent the consensus of the industry, and that the vast majority of the industry will embrace them.” (8)

The impact of this organization to the security industry is significant. While it seems to be well intentioned, the potential danger is exemplified in the potential IE hole, explained above, that is yet to be patched. The following are some short-term proposals from the organization:

“Report and address security vulnerabilities thoroughly and expeditiously.

Provide users with a reasonable opportunity to protect their systems against newly announced security vulnerabilities, by observing a 30-day grace period before disclosing details for exploiting the vulnerabilities.

Exercise due diligence when developing security tools, to limit their use to only lawful purposes.” (8)

Conclusions

The process of software, system, and network creation has the built in correction and update system, known within the industry as the patch process. We can continue to expect the “ship now, fix later” process. To compound the issue, with the pressures from political and economic situations around the world, we can continue to expect shortages of competent security professions, increased attacks on our infrastructure, and even more demands to provide the services required by an E business driven economy.

The new initiatives to help improve this process, such as certification and the formation of organizations are welcomed. Participation of the entire community is going to be key to the success of these initiatives. Not only participation by patching, and keeping patched the systems we maintain, but also helping to assist in patching the patch process.

References

- 1) "Demands on IT managers is jeopardizing security." 29 Nov. 2001.
URL: <http://www.activis.com/en/contentnews/news29-11-01.html> (12 Dec. 2001).
- 2) Olson, Geoff. "SHODDY SOFTWARE."
URL: <http://www.geocities.com/SoHo/Gallery/3452/hitset.htm> (12 Dec. 2001).
- 3) Somogyi, Stephan. "Security lapses must be penalized." 16 Mar. 2001.
URL: <http://www.zdnetindia.com/techzone/enterprise/stories/16935.html>
(12 Dec. 2001).
- 4) Schneier, Bruce. "Are you ready for a cyber-UL?" 2 Jan. 2001.
URL: <http://www.zdnet.com/zdnn/stories/comment/0,5859,2669708,00.html>
(12 Dec. 2001).
- 5) Center for Internet Security.
URL: <http://www.cisecurity.org> (12 Dec. 2001).
- 6) Morgan, Gareth. "Microsoft 'patch-bundling' faces hurdles." 9 Oct. 2001.
URL: <http://news.zdnet.co.uk/story/0,,t269-s2096745,00.html> (8 Dec. 2001).
- 7) "2001-11-26 Security Note: File extensions spoofable in MSIE download dialog". Oy Online Solutions Ltd. 11 Nov. 2001.
URL: http://www.solutions.fi/index.cgi/news_2001_11_26?lang=eng
(12 Dec. 2001).
- 8) "Organization to Propose Vulnerability-Handling Standards". Microsoft.
Nov. 2001.
URL: <http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/news/standard.asp> (12 Dec. 2001).



Upcoming SANS Training

[Click Here for a full list of all Upcoming SANS Events by Location](#)

SANS Tampa - Clearwater 2017	Clearwater, FLUS	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Network Security 2017	Las Vegas, NVUS	Sep 10, 2017 - Sep 17, 2017	Live Event
SANS Dublin 2017	Dublin, IE	Sep 11, 2017 - Sep 16, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MDUS	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, DK	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, GB	Sep 25, 2017 - Sep 30, 2017	Live Event
Data Breach Summit & Training	Chicago, ILUS	Sep 25, 2017 - Oct 02, 2017	Live Event
Rocky Mountain Fall 2017	Denver, COUS	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS SEC504 at Cyber Security Week 2017	The Hague, NL	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Oslo Autumn 2017	Oslo, NO	Oct 02, 2017 - Oct 07, 2017	Live Event
SANS DFIR Prague 2017	Prague, CZ	Oct 02, 2017 - Oct 08, 2017	Live Event
SANS Phoenix-Mesa 2017	Mesa, AZUS	Oct 09, 2017 - Oct 14, 2017	Live Event
SANS October Singapore 2017	Singapore, SG	Oct 09, 2017 - Oct 28, 2017	Live Event
SANS AUD507 (GSNA) @ Canberra 2017	Canberra, AU	Oct 09, 2017 - Oct 14, 2017	Live Event
Secure DevOps Summit & Training	Denver, COUS	Oct 10, 2017 - Oct 17, 2017	Live Event
SANS Tysons Corner Fall 2017	McLean, VAUS	Oct 14, 2017 - Oct 21, 2017	Live Event
SANS Tokyo Autumn 2017	Tokyo, JP	Oct 16, 2017 - Oct 28, 2017	Live Event
SANS Brussels Autumn 2017	Brussels, BE	Oct 16, 2017 - Oct 21, 2017	Live Event
SANS Berlin 2017	Berlin, DE	Oct 23, 2017 - Oct 28, 2017	Live Event
SANS San Diego 2017	San Diego, CAUS	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS Seattle 2017	Seattle, WAUS	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS Gulf Region 2017	Dubai, AE	Nov 04, 2017 - Nov 16, 2017	Live Event
SANS Miami 2017	Miami, FLUS	Nov 06, 2017 - Nov 11, 2017	Live Event
SANS Amsterdam 2017	Amsterdam, NL	Nov 06, 2017 - Nov 11, 2017	Live Event
SANS Milan November 2017	Milan, IT	Nov 06, 2017 - Nov 11, 2017	Live Event
Pen Test Hackfest Summit & Training 2017	Bethesda, MDUS	Nov 13, 2017 - Nov 20, 2017	Live Event
SANS Paris November 2017	Paris, FR	Nov 13, 2017 - Nov 18, 2017	Live Event
SANS Sydney 2017	Sydney, AU	Nov 13, 2017 - Nov 25, 2017	Live Event
SANS San Francisco Fall 2017	OnlineCAUS	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced