Global Information Assurance Certification Paper

Drowning in Patches!

GSLC V 1.0
Ray Rodman
12/6/2003

Abstract

Patching deals with fixing vulnerabilities (or flaws) in vendor software. This is necessary since vulnerabilities can be used to attack a system and expose important company information to misuse. When vulnerabilities are found, vendors develop fixes that are made available to the public, usually by placing the patch on their website so the user can download the fix and install it. By installing the fix (or patch), the vulnerability in the user's software is repaired and can no longer be exploited.

With the number of vulnerabilities increasing every year, the numbers of patches that must be managed are also increasing. According to the CERT Coordination Center of Carnegie Mellon University in Pittsburg, the number of reported vendor software vulnerabilities has grown dramatically over the last five years. In 1998, there were just 262 software vulnerabilities reported, but by 2002, that number had grown to 4,129. Through three quarters in 2003, with 2,982 vulnerabilities reported, the pace of reported vulnerabilities continues unabated.[1]

Clearly, most threats against systems can be avoided by patching vulnerable systems. It all sounds simple, but appearances can be deceiving. Due to the exponential growth of vulnerabilities over the last five years, the magnitude of patches needed to fix those vulnerabilities, has itself become an issue.

The Cost to Business

In January, 2003, the Slammer worm was released on the computing world. Amazingly, within in 10 minutes Slammer was pandemic as 90 percent of all vulnerable machines in the world were infected. Even Microsoft was badly infected.[2] Furthermore, according to Scott Berinato in CIO, "ISP networks had collapsed; several DNS servers were overwhelmed; airlines had canceled flights; ATM machines refused to hand out money. In Canada, a national election was delayed."[3] Can you imagine the reaction in this country if a national election had to be delayed due to computer problems?

Disruptions of this magnitude obviously carry a high cost, which was even more clearly demonstrated in August, 2003, when two crippling viruses (Blaster and SoBig) were released on the computing world. According to BusinessWeek, "Worldwide, 15% of large companies and 30% of small companies were affected by SoBig…" The article goes on, "Market researcher Computer Economics Inc.

[1] "CERT/CC Statistics 1988-2003," Carnegie Mellon Software Engineering Institute, 17 Oct. 17 2003. URL: http://www.cert.org/stats/cert_stats.html Accessed Dec. 2, 2003
[2] Berinato, Scott. "FrankenPatch." CIO. November 1, 2003. 100-110
[3] Berinato, Scott. "FrankenPatch." CIO. November 1, 2003. 100-110

estimates damage will total $2 billion—one of the costliest viruses ever. All told, damage from viruses may amount to more than $13 billion this year."[4] Damages of this magnitude can put a company's future viability at risk, and is a huge drain on the nation's economy.

The costs of dealing with and recovering from exploited vulnerabilities are great, but they are not the only costs to an organization. The cost of preventing exploitation of vulnerabilities can also be significant. According to SC Magazine, "some estimates from analysts firms show that costs per year to patch 1,000 nodes manually run about $300,000."[5] The process of identifying available patches, deciding which patches to implement in your computing environment, testing those patches, installing all selected patches on all systems, and finally verifying installation can be overwhelming due to the ever growing number of vulnerabilities identified every year (4,129 in 2002).[6]

Billions of dollars could have been saved in 2003 alone if organizations had implemented available patches for Slammer and Blaster. Slammer appeared six months after a patch was available. The lead time for Blaster was much shorter, with the Blaster worm coming out less than 30 days after the vulnerability and patch were announced. This reduction in the time between a vulnerability becoming known and when it is exploited adds to the costs of patch management and the urgency of implementing patches as soon as they become available. According to SC Magazine, the

> Internet Security Systems' X-Force team has released a report that has found the gap between system/software vulnerabilities and attack methods getting shorter. That is, the techniques hackers are using to hit corporate infrastructures are relying more and more on the unpatched systems left open for attack.[7]

Unfortunately, many companies have not seen the need to translate these concerns into real investments in security processes, staffing, and technology. This is particularly true in a tight economy where investments tend to focus on those areas that yield the most profit.

Is Patching the Answer?

According to a growing segment of people in the industry, patching no longer works. CNET News.com reports that, "The ability of the MSBlast worm to spread has underscored that today's methods of patching security flaws ... is too time-

[4] Hamm, Steve; Greene, Jay; Edwards, Cliff; and Kerstetter, Jim. "Epidemic." BusinessWeek, Sept 8, 2003. 28-34.
[5] Armstrong, Illena. Editorial. SC Magazine. August, 2003. 9
[6] "CERT/CC Statistics 1988-2003," Carnegie Mellon Software Engineering Institute, 17 Oct. 17 2003. URL: http://www.cert.org/stats/cert_stats.html Accessed Dec. 2, 2003
[7] Armstrong, Illena. Editorial. SC Magazine. August, 2003. 9

consuming to react to critical vulnerabilities."[8] For instance, the University of Florida had hundreds of systems infected by Blaster, despite a broad initiative by the school to lock down its systems with patches.[9]

In the last year, the sheer number of patches has overwhelmed IT managers in many companies, placing network security at greater risk. The Blaster worm "…highlighted the enormous challenge companies face in keeping their systems up to date with patches for vulnerabilities…"[10] Whether because of a lack of understanding the risk involved, poor management practices, low priority, lack of funds, or for other reasons, the lesson learned by many was that patching couldn't be relied upon to keep computers secure.

Recently, the idea of patch management systems to automate patches has received a lot of attention. Many people see a need to patch very aggressively as the best way to avoid the increasing frequency of vulnerability exploits. The intent of patch management systems is to reduce costs through automation and human error by making the installation of patches a no-brainer. As noted earlier it is estimated that manually patching 1,000 nodes costs approximately $300,000."[11] Obviously manually patching that many nodes is also error prone, so there is no guarantee that fixes have been successfully implemented.

Software can be used to eliminate, or at least reduce human involvement by automating the process of finding, downloading, applying patches and verifying that patches have been successfully installed.[12] Several vendors now offer software for this purpose. However, automated updating isn't foolproof either since patches aren't as simple as click-and-fix. For one, not all patches work as advertised, or they may not work on all systems, so testing is still necessary to assure quality. Patching also requires that servers be taken out of service long enough for the fix to be applied, and this affects production work. The more patches the greater the potential for problems, and the more downtime needed to do the installations.

Another thought is that patch management is a failing strategy. Those supporting this view argue that all we need to do is look at Slammer for proof. This well known vulnerability was around for at least eight months before it was exploited and a patch was available six months before it was exploited. Yet, many companies simply failed to prepare. In his opinion article on patch management, Phil Hollows, VP of Security Products for OpenService states, "Patches cannot be relied upon to deliver effective front-line security, because they simply aren't

---

[8] Lemos, Robert. "Worm's spread shows holes in patch system." CNET News.com. 12 Aug. 2003 URL: http://news.com.com/2100-1002-5062832.html Accessed Dec. 2, 2003

[9] Lemos, Robert. "Worm's spread shows holes in patch system." CNET News.com. 12 Aug. 2003 URL: http://news.com.com/2100-1002-5062832.html Accessed Dec. 2, 2003

[10] Vijayan, Jaikumar. "Patching Becoming a Major Resource Drain for Companies." Computerworld. August 18, 2003. 1, 15

[11] Armstrong, Illena. Editorial. SC Magazine. August, 2003. 9

[12] Berinato, Scott. "Patch and Pray." CSO. August 2003. 34-40

applied in a consistent, effective and timely fashion."[13] He goes on to say that proactive network security management is needed. This would involve correlating data from multiple sensors, including Intrusion Detection Systems (IDS), firewalls and anti-virus to look for patterns to detect threats in real time.[14] This strategy sounds good, but it is not a simple task. IDS systems are notorious for setting off false alarms, and correlating data from multiple systems requires significant automation and fine tuning to be manageable. Some vendors, such as OpenSource, Inc. are developing applications to help with the correlation of data, but the concept is still new and needs to be proven in the real world. Even if this approach (which appears to hold some promise) can be implemented, installing patches will still be a necessary part of the overall process. Proactive network security management may be able to delay the need for immediate patch installation, but ultimately, the fix will still be necessary.

Conclusion

The ultimate solution to the problem of patching is to eliminate vulnerabilities before they become vulnerabilities. Vendors need to provide higher quality products to their customers instead of rushing products to market before they have been sufficiently tested. Improving software quality would reduce the need for patches. Vendors and customers alike would benefit. Vendors could spend more of their time and money on developing new or enhanced products in place of developing, testing and distributing patches. Purchasers of software could reduce the overhead needed to manage patch installation processes to fix problems.

Unfortunately, software quality problems seem to be with us for the foreseeable future, and until that changes, patching is going to remain a part of our lives as the best available option. Therefore, we must focus on improving all aspects of the patching process.

As we have seen, manual patch processes are not workable for large organizations in today's environment. There are simply too many patches and when this is applied to large network environments, the costs are prohibitive. Some automation is not only desirable, it is necessary for many aspects of the patching process. However, full automation doesn't appear to be the answer either due to the limitations described earlier. Lastly, although network security event management solutions appear to hold promise for easing the urgency of patching in the future, this technology still needs to be proved in the real world.

That leaves us with the need to automate what we can, and the need to develop policies and procedures for what can't be automated. Automation should include notification of all new patches, and a process for pushing patches to all systems

[13] Hollows, Phil. "Is Patch Management a Failing Strategy?" SC Infosec Opinionwire. Aug. 2003 URL: http://www.infosecnews.com/opinion/2003/08/27_02.htm Accessed Dec. 2, 2003
[14] Hollows, Phil. "Is Patch Management a Failing Strategy?" SC Infosec Opinionwire. Aug. 2003 URL: http://www.infosecnews.com/opinion/2003/08/27_02.htm Accessed Dec. 2, 2003

once the decision has been made to install the patch. Along with this, the decision process for deciding which patches to install must be clearly defined. Who (individual or group of people) will be accountable for making the decision to install a patch? This person or group should also be responsible for deciding how frequently patches are to be applied. Daily, weekly, monthly, or some combination based on priority of the fix? As well, test environments (for larger organizations, dedicated environments may be necessary) need to be set up so patches can be thoroughly tested before installation. Finally, a timeline should be agreed upon and established as a company priority. Recently, we have seen the time lapse between the recognition of a vulnerability to the exploitation of that vulnerability reduced to as little as 30 days. This is probably the outside limits for implementing critical patches in today's environment.

Hackers know that many organizations delay patching, so known vulnerabilities become an open invitation to target them, and hackers do. This will not change, so for now, it is incumbent upon organizations that they take patching seriously and make it a priority. Companies can't afford to wait for better approaches to come along before acting.

List of References

"CERT/CC Statistics 1988-2003," Carnegie Mellon Software Engineering Institute, 17 Oct. 17 2003. URL: http://www.cert.org/stats/cert_stats.html Accessed Dec. 2, 2003

Berinato, Scott. "FrankenPatch." CIO. November 1, 2003. 100-110

Hamm, Steve; Greene, Jay; Edwards, Cliff; and Kerstetter, Jim. "Epidemic." BusinessWeek, Sept 8, 2003. 28-34.

Armstrong, Illena. Editorial. SC Magazine. August, 2003. 9

Lemos, Robert. "Worm's spread shows holes in patch system." CNET News.com. 12 Aug. 2003 URL: http://news.com.com/2100-1002-5062832.html Accessed Dec. 2, 2003

Vijayan, Jaikumar. "Patching Becoming a Major Resource Drain for Companies." Computerworld. August 18, 2003. 1, 15

Berinato, Scott. "Patch and Pray." CSO. August 2003. 34-40

Hollows, Phil. "Is Patch Management a Failing Strategy?" SC Infosec Opinionwire. Aug. 2003 URL: http://www.infosecnews.com/opinion/2003/08/27_02.htm Accessed Dec. 2, 2003

Last Updated: July 27th, 2017

Upcoming Training

SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS New Orleans MGT512	New Orleans, LA	Aug 21, 2017 - Aug 25, 2017	Community SANS
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
Community SANS New York MGT512	New York, NY	Aug 28, 2017 - Sep 01, 2017	Community SANS
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Community SANS Toronto MGT512	Toronto, ON	Sep 18, 2017 - Sep 22, 2017	Community SANS
Community SANS Columbus MGT512	Columbus, OH	Sep 25, 2017 - Sep 29, 2017	Community SANS
SANS Oslo Autumn 2017	Oslo, Norway	Oct 02, 2017 - Oct 07, 2017	Live Event
SANS Tysons Corner Fall 2017	McLean, VA	Oct 14, 2017 - Oct 21, 2017	Live Event
Community SANS Banff MGT512	Banff, AB	Oct 23, 2017 - Oct 27, 2017	Community SANS
SANS San Diego 2017	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	Live Event
Community SANS Memphis MGT512	Memphis, TN	Nov 06, 2017 - Nov 10, 2017	Community SANS
SANS San Francisco Winter 2017	San Francisco, CA	Nov 27, 2017 - Dec 02, 2017	Live Event
SANS Cyber Defense Initiative 2017	Washington, DC	Dec 12, 2017 - Dec 19, 2017	Live Event
SANS Security East 2018	New Orleans, LA	Jan 08, 2018 - Jan 13, 2018	Live Event
Northern VA Winter - Reston 2018	Reston, VA	Jan 15, 2018 - Jan 20, 2018	Live Event
SANS Miami 2018	Miami, FL	Jan 29, 2018 - Feb 03, 2018	Live Event
SANS Southern California- Anaheim 2018	Anaheim, CA	Feb 12, 2018 - Feb 17, 2018	Live Event
SANS OnDemand	Online	Anytime	Self Paced
SANS SelfStudy	Books & MP3s Only	Anytime	Self Paced