MAINTAINING VULNERABLE SERVERS
WHAT’S YOUR WINDOW OF EXPOSURE?
Patch Management Difficulties

System administrators, also called “security or server administrators,” are tasked with managing the overall confidentiality, integrity, and availability of company servers. Virtualization and the growing adoption of different cloud technology implementations add complexities that blur perceived boundaries. The inherent conflict here is that while the responsibility for protecting and defending company assets lies in a different IT group, the system administrators' actions or inactions have a significant effect on security.

Despite prevalent information on the effects of data breaches, some administrators either prefer or are forced to keep their servers and endpoints unpatched. Enterprises know that attacks against their networks can be launched anytime. Why then do administrators leave their systems vulnerable?

**BUSINESS CONTINUITY.** For systems that perform mission-critical roles and require 100% uptime, restarts required for updates to take effect can translate to significant business losses, pushing administrators to delay deployment.

**QUALITY ASSURANCE.** Testing patches may take a few minutes to a month, more likely so if these involve vulnerabilities and hundreds of different system configurations. Virtualized environments and cloud-based applications may also pose additional challenges.

**ROLLBACKS AND INTENTIONAL DELAYS.** Administrators are likely to delay the deployment rollout of patches that proved unstable or caused unexpected behaviors in the environment, especially if recovery after a disaster will demand huge amounts of time and effort.

**EMERGENCY (OUT-OF-BAND) PATCHES.** Out-of-band updates can come at inconvenient times such as when administrators are focusing on high-priority projects, unable to take affected assets that play mission-critical functions offline, or have taken off for the holidays such as when Microsoft released its yearend update on December 29, 2011.

**NO AVAILABLE PATCHES.** Developing patches may take vendors days to weeks or, in some instances, even years. Some vendors or developers may no longer support legacy systems such as several versions of Windows 2000 and Windows Server 2003, for which Microsoft ended mainstream support.

System administrators have to make difficult judgment calls that may put their company's data centers and networks at risk. Server OSs—a vital part of high-functioning data centers—in particular, are not immune to vulnerabilities. Figure 1 shows the most widely used server OSs according to the Common Vulnerabilities and Exposures database and the percentage of severity of the reported vulnerabilities for each.

“There are so many unpatched systems... [that] it's easier to utilize a well-known vulnerability and still reach a big enough customer base.”

—Raimund Genes, “Zero-Day Vulnerabilities Risk Overblown”
Risks of Keeping Servers Vulnerable

DISRUPTIVE MALWARE

DOWNAD, also known as “Conficker,” caused heavy LAN traffic in infected networks. This effect is a by-product of DOWNAD’s routines but is notable due to how easy infection could have been avoided.

DOWNAD worms spread throughout a network by exploiting the Server Service vulnerability (CVE-2008-4250), for which a patch has been made available since 2008. However, based on Trend Micro™ Smart Protection Network™ data for December 2011, DOWNAD remains the most common malware found in Windows-based servers. It is also specifically found among companies that belong to the banking, financial, insurance, and healthcare sectors.

OTORUN worms, so named for their propensity to spread through removable drives, are also on this list of common network infectors. A particular variant of this worm, for instance, exploits the LNK vulnerability, which can result in remote code execution. Traces of these worms have been found among organizations in the telecommunications and manufacturing industries.

CYBERCRIME, DATA BREACHES, AND TARGETED ATTACKS

Socially Engineered/Client-Side Attacks

In our annual security report, we observed that the exploits in 2011 were now targeted, original, and well-controlled. Furthermore, cybercriminals find zero-day vulnerabilities expensive, so it is easier and cheaper for them to use well-known vulnerabilities as long as they use effective social engineering tactics.

The most common exploits in these kinds of attacks take advantage of OS and application vulnerabilities. For instance, around December 2011, Trend Micro analyzed a PDF that came with an email. The PDF appeared be an “Employee Satisfaction Survey” but actually carried an exploit for CVE-2011-2462 that installed a backdoor.

Server-Side Attacks

Web server and web applications contain vulnerabilities that permit cybercriminals to access parts of a company’s servers that they should not be able to. Server-side attacks like cross-site scripting attacks, SQL injections, and others take advantage of vulnerabilities that can be used to infiltrate company assets. For instance, cybercriminals used vulnerabilities found in Apache HTTP Server (CVE-2011-3192) to conduct denial-of-service attacks that do not require large amounts of traffic to take down sites.

FINANCIAL LOSS

Enterprises stand to lose confidential information from trade secrets to customer databases that can then be sold in underground forums or used in subsequent and more damaging attacks. Also, these corporate victims have to inevitably spend resources—both time and money—to deal with intrusions. In addition, enterprises will have to deal with repairing a damaged brand name or image.

“Start with the cost of notifying victims, tack on the expense of lawsuits, implementing new security measures and ongoing marketing to repair a damaged reputation, and some businesses never recover.”

—Attorney General Mckenna on the TJX data breach, 2009
Vulnerability Shielding

Vulnerability shielding, also called “virtual patching,” is a security or patch management strategy that can protect OSs, applications, and endpoints from attacks leveraging software vulnerabilities.

Vulnerability shielding works on the premise that exploits take a specific or definable network path to and from an application in order to use a vulnerability. It is, therefore, possible to manipulate the network layer through rules to control the communications being made to the targeted software.

Instead of immediately altering a vulnerable program, vulnerability shielding enables system administrators to scan for deviations from typical protocols used and suspicious traffic, effectively preventing exploits from being of any use. Administrators can do so without the need to shut down systems, minimizing downtime and allowing them to conduct emergency patching on the fly and to wait for the regular patching schedule.

Solutions with vulnerability shielding capabilities like Deep Security and OfficeScan with the Intrusion Defense Firewall (IDF) plug-in can deliver the necessary protection to minimize the vulnerability gap.
TREND MICRO™

Trend Micro Incorporated (TYO: 4704; TSE: 4704), a global cloud security leader, creates a world safe for exchanging digital information with its Internet content security and threat management solutions for businesses and consumers. A pioneer in server security with over 20 years’ experience, we deliver top-ranked client, server and cloud-based security that fits our customers’ and partners’ needs, stops new threats faster, and protects data in physical, virtualized and cloud environments. Powered by the industry-leading Trend Micro™ Smart Protection Network™ cloud computing security infrastructure, our products and services stop threats where they emerge—from the Internet. They are supported by 1,000+ threat intelligence experts around the globe.

TRENDLABS™

TrendLabs is a multinational research, development, and support center with an extensive regional presence committed to 24 x 7 threat surveillance, attack prevention, and timely and seamless solutions delivery. With more than 1,000 threat experts and support engineers deployed round-the-clock in labs located around the globe, TrendLabs enables Trend Micro to continuously monitor the threat landscape across the globe; deliver real-time data to detect, to preempt, and to eliminate threats; research on and analyze technologies to combat new threats; respond in real time to targeted threats; and help customers worldwide minimize damage, reduce costs, and ensure business continuity.