Gartner Research

Publication Date: 17 October 2006 ID Number: G00144061

Responsible Vulnerability Disclosure: Guidance for Researchers, Vendors and End Users

Amrit T. Williams, John Pescatore, Paul E. Proctor

Vulnerability disclosure is a process executed primarily between security researchers (both commercial and independent) and software product vendors. When a vulnerability is found, the researcher notifies the vendor, the vendor creates a patch, and end-user organizations test and deploy the patch. “Responsible disclosure” means that the researcher and vendor work together diligently and ethically to produce a timely patch to reduce the risk as much as possible for the end-user organizations. Gartner provides guidance for responsible disclosure to researchers, independent software vendors (ISVs) and end users.

Key Findings

- Attackers looking to exploit vulnerabilities in IT will focus their efforts in the area in which a critical vulnerability may exist, increasing the potential that the vulnerability is identified and an exploit made available.
- When a vulnerability is publicly announced, attackers and researchers generally find more vulnerabilities in the product(s) or similar vulnerabilities in other products soon after.
- It is a common practice for hackers to reverse-engineer both patches to better understand how to exploit vulnerabilities, and this can be extended to security product signatures. Security vendors that provide "zero-day" protection for their clients, prior to release of a patch, can put the broader IT community at risk if they don't take precautions.
- IT vendors that do not provide adequate information on the nature of a vulnerability will impact the ability of their user base to make decisions on how to proceed with a work-around, patch or deployment of a new version. This delays patching and increases risk.
- End-user IT organizations absorb most of the risk if disclosure is done irresponsibly, and they have limited influence over the process. Enterprises should not buy security products from companies that do not practice responsible disclosure. There are also situations that arise in which disclosure can and should impact how an organization reacts.

Predictions

- Through 2010, active zero-day attacks will increase by 10% (0.8 probability).

- Through 2010, reducing vulnerabilities in commercially acquired products and services by just 50% will reduce configuration management and incident response costs by 75% each (0.7 probability).
- By year-end 2008, application security will become an important evaluation criterion, weighted as high as system functionality (0.7 probability).

Recommendations

- Researchers and ISVs should work together using responsible disclosure guidelines.
- End users should have visibility into events when disclosure “goes wrong” and respond appropriately.

ANALYSIS

Publicity over vulnerabilities in software products is a double-edged sword. Making vulnerabilities public has, unfortunately, proved necessary to spur some software vendors to invest in better software development, patch production and patch distribution processes. However, it has also enabled attackers to more quickly produce exploits.

Security researchers should practice responsible disclosure by providing all necessary information to the ISV and allowing an appropriate amount of time for the ISV to respond. ISVs have responsibility to their user base to provide adequate information that allows their clients to make the appropriate decisions about implementation of a work-around, distribution of a patch, or upgrade to a new version.

End-user IT organizations absorb most of the risk if disclosure is done irresponsibly because they will have to deal with attacks that occur before patches are available. Enterprises have no influence over the disclosure practices of attackers, but by buying vulnerability assessment or intrusion prevention products only from vendors that practice responsible disclosure, enterprises can drive honest companies to stay honest. In addition, situations arise in which disclosure can and should impact how an organization reacts.

Responsible disclosure is good for security researchers, ISVs and, most importantly, the enterprises and end users of these products. Security researchers and ISVs must follow responsible disclosure guidelines. Views vary on how organizations should handle vulnerability disclosure. We define guidelines for the responsible disclosure of vulnerabilities for security researchers and ISVs, as well as provide guidance for end users affected by this process.

Vendor Notification

Security researchers must notify the vendor and provide all information needed to identify the vulnerability, and reproduce the exploit or provide the proof of concept. The security researcher must allow sufficient time for the vendor to acknowledge receipt of the information before making any information public. Sufficient time for vendor acknowledgment is typically 30 days.

If the vendor requests a reasonable amount of additional time (on the order of another four to six weeks), no information should be released. Ideally, the security researcher and ISV would work to resolve the issue; however, researchers argue that many ISVs do not respond or ignore their submissions. Some researchers feel compelled to announce that a vendor's product contains a critical vulnerability prior to a work-around, patch or upgrade being available; generally, they will not name the product, just the vendor — this practice provides no benefit to the IT community because there is no actionable advice. At no point prior to the vendor publicly releasing a patch or work-around should detailed information on the product or vulnerability be made public.

Initial Public Vulnerability Release

Many security researchers face vendors that are nonresponsive, will not provide an estimated time of arrival (ETA), or are unwilling to work with the security research community. The longer a vulnerability remains unresolved, the greater the potential that it will be found and exploited for malicious purposes. Security researchers should allow six months for the vendor to provide an ETA for a work-around, patch or upgrade. If the vendor has not responded with resolution or an acceptable ETA for resolution (potentially six to nine months) within that time, then information on the vulnerability should be provided to the greater security research community to ensure that defensive mechanisms can be properly implemented.

Detailed Vulnerability, Remediation and Mitigation Information

ISVs have responsibility to their user base to provide adequate information that allows their clients to make the appropriate decisions about implementation of a work-around, distribution of a patch, or upgrade to a new version. ISVs must provide information on all vulnerabilities, their severity, existence of known threats, work-arounds and any other information that an enterprise would need to make an informed decision to deal with the vulnerable condition. ISVs should also update patch release information when conditions change after the patch is released. Additionally, ISVs should properly credit the security researcher with discovering the vulnerability.

Guidance for Security Researchers

Provide all necessary information to the ISV and obtain a positive indication that the appropriate function within the vendor has received the information. An appropriate amount of time (typically at least 30 days) should be allowed for the ISV to respond before releasing any information, even information without details. If the vendor requests a reasonable amount of additional time (another four to six weeks), no information should be released. Work closely with the vendor to ensure a timely response and be prepared to publicly announce the vulnerability details when the vendors has provided a patch, work-around or software update, but not before. Exploit code should never be released.

Guidance for ISVs

Provide a well-publicized means of accepting vulnerability information from researchers, as well as a published policy for how your organization will respond and work with security researchers. Researchers that follow responsible reporting protocols should be credited when the patch is publicly released. ISVs should actively include the vulnerability research community in alpha and beta testing cycles of their products.

Guidance for End-User IT Organizations

There's little that an end-user organization can do to affect who finds or discloses vulnerabilities. However, these events are recognizable in the press and through vulnerability information sources. Remember that no patch will be available. Organizations must respond to these occurrences by absorbing the available information as soon as possible and adjusting their controls — including reconfiguring firewall, intrusion detection system, intrusion prevention system, security information and event management, and network behavior analysis technologies — to detect suspicious behavior or block affected protocols if possible. Limit the use of affected applications where they are not mission-critical.

Determine where your organization fits in its approach to disclosure so you can make a good assessment of available information. If you are a larger organization, determine how you will use details included in disclosures to make good decisions for remedial actions.

Organizations should not conduct business with vendors or security research companies that do not follow responsible disclosure. These entities must not be allowed to manipulate, intentionally or not, enterprise security postures.

A preferred list is a special list that a vendor would keep of large customers who would get special attention and potentially early notification of vulnerabilities. Aside from the obvious ethical issue with parity, there's a risk of exposure when vulnerability data is made available to anyone outside the vendor. Most ISVs have shunned preferred lists because of this risk, but mostly because they are difficult to manage, and once knowledge of a list gets out, everyone wants to be on it. Then it ceases to be “preferred.” The bottom line is they don't make business sense. In fact,

Sun Microsystems and Cisco Systems report that they use only public information to remediate their own enterprises against vulnerabilities. Don't count on, look for or demand to be on preferred lists for vulnerability information from your primary ISVs.

Third-Party Patches

Some third parties produce patches for popular software. These patches are typically available free or sold through services with the intent of filling the gap between disclosure and the availability of the vendor patch. Most of the organizations that produce these patches are also vulnerability research organizations, so there is an inherent conflict of interest. Gartner does not recommend using third-party patching for security issues. The cure may be worse than the disease: Third-party patches can create havoc in a large organization because of inconsistent quality, which may result in service or application disruption, limited ability to manage them remotely and the need to uninstall them when the vendor-approved patch is available. In the worst-case scenario, they may contain backdoors or other malicious software.

RECOMMENDED READING

"Improve IT Security With Vulnerability Management"

"Identifying and Solving Vulnerability Management Weak Spots"

"Visibility and Control Are Key to Managing IT Security Vulnerabilities"

REGIONAL HEADQUARTERS

Corporate Headquarters
56 Top Gallant Road
Stamford, CT 06902-7700
U.S.A.
+1 203 964 0096

European Headquarters
Tamesis
The Glanty
Egham
Surrey, TW20 9AW
UNITED KINGDOM
+44 1784 431611

Asia/Pacific Headquarters
Gartner Australasia Pty. Ltd.
Level 9, 141 Walker Street
North Sydney
New South Wales 2060
AUSTRALIA
+61 2 9459 4600

Japan Headquarters
Gartner Japan Ltd.
Aobadai Hills, 6F
7-7, Aobadai, 4-chome
Meguro-ku, Tokyo 153-0042
JAPAN
+81 3 3481 3670

Latin America Headquarters
Gartner do Brazil
Av. das Nações Unidas, 12551
9° andar—World Trade Center
04578-903—São Paulo SP
BRAZIL
+55 11 3443 1509

Gartner