



Codenomicon whitepaper:

Unknown Vulnerability Management

- Anna-Maija Juuso and Ari Takanen -



- 1** Introduction
- 2** Unknown Vulnerabilities Enable Zero-Day Attacks
- 3** Discover Security Issues Proactively, Don't React to Them
- 4** Codenomicon Defensics for Unknown Vulnerability Management
- 5** How to Defend Your Systems
- 6** Conclusion

CODENOMICON Ltd. | info@codenomicon.com | www.codenomicon.com

Tutkijantie 4E | FIN-90570 OULU | FINLAND | +358 424 7431
10670 North Tantau Avenue | Cupertino, CA 95014 | UNITED STATES | +1 408 252 4000

PREEMPTIVE SECURITY AND ROBUSTNESS TESTING SOLUTIONS

1 Introduction

The greatest security challenge for enterprises today is discovering unknown vulnerabilities hiding in software. Software release cycles are getting faster and new technologies are increasingly complex, creating a perfect breeding ground for security-related bugs. New patches are released every week, each requiring immediate attention. The maintenance downtime alone is expensive. Not to mention the costs of ad-hoc deployment, which is also prone to errors. At the same time, a growing share of vulnerabilities is never disclosed publicly. Instead, they are sold and distributed within underground hacker communities. Companies can no longer afford to wait for patch releases from vendors, nor can they rely on user communities to find and report these bugs. Thus, they need to find new proactive ways to protect their products and services.

*It's what you don't know
that makes you vulnerable*

2 Unknown Vulnerabilities Enable Zero-Day Attacks

Unknown vulnerabilities are exploitable bugs hidden in software code. In contrast to known disclosed vulnerabilities with available patches and updates, vendors are unaware of the existence of these unknown bugs, and therefore they are not prepared to provide fixes for them. Vulnerabilities in customer-facing applications provide the easiest and most frequently used way for hackers to attack an enterprise. Thus, finding and fixing vulnerabilities in your own and outsourced code development should be a top priority. There is no use in trying to protect an impaired system or application with firewalls and anti-virus software. These merely add to the complexity of the system, and complexity is always a threat, because it increases the attack surface of the system. For example, if hackers manage to compromise another user in your VPN network, they gain direct entry into your network. Indeed, the more complex your system or network is the more hidden attack surfaces there are. By recording actual traffic in your network and examining it, you can reveal vulnerable interfaces that you were not aware of and even discover possible zero-day exploits in action.

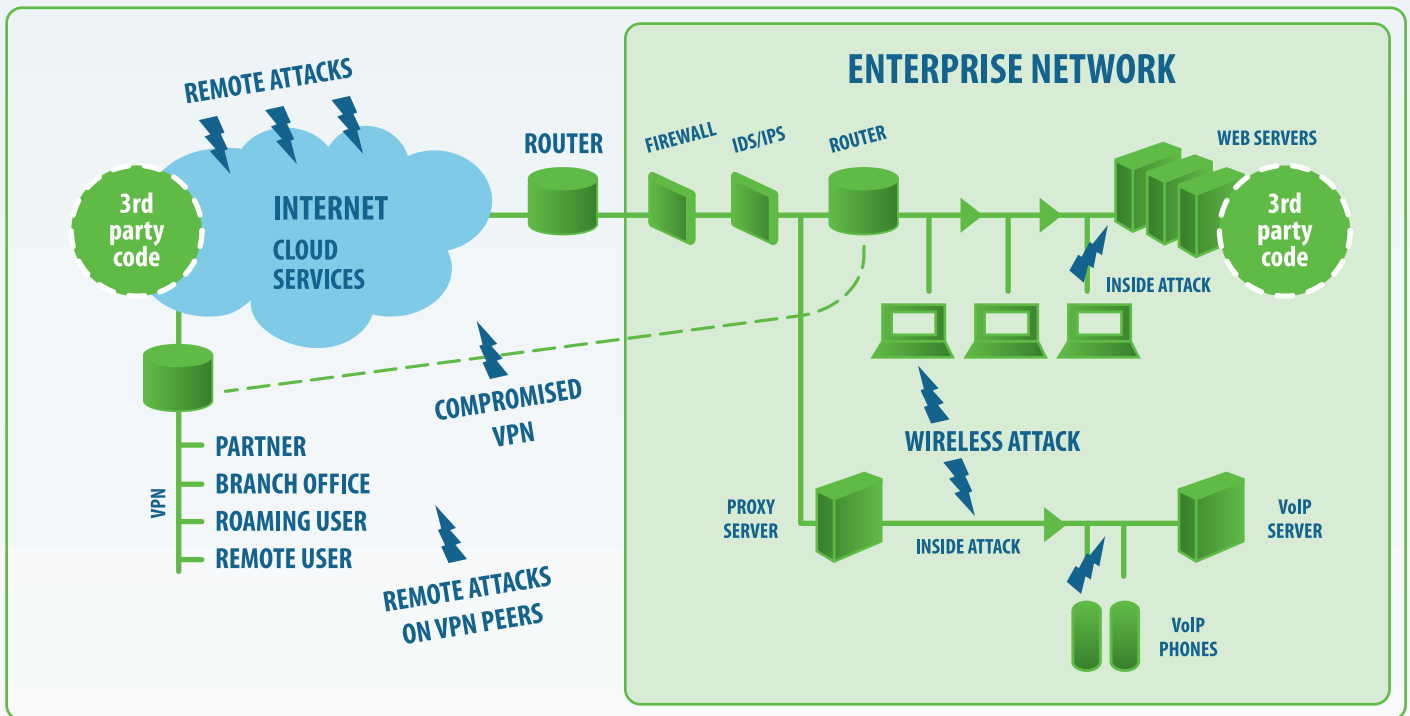


Figure 1: Threats within an Enterprise Network

3

Discover Security Issues Proactively, Don't React to Them

Unknown vulnerabilities can cause companies a lot of havoc. Attacks against unknown vulnerability can go undetected and once the attack is discovered, the repair process tends to be slow, because there are no ready patches or updates. All the time, customers are unable to access your service, or even worse: their safety is endangered. Similarly, installing a new patch causes downtime, meaning your customers are not able to access your services. Moreover, all the downtime and problems are bad to your company reputation and ultimately your sales. Wouldn't it be much better to discover security issues proactively and then deploy all the fixes in one big push? By finding and fixing vulnerabilities proactively, you also have time to verify the fixes.

4

Codenomicon Defensics for Unknown Vulnerability Management

Unknown Vulnerability Management is the process of proactively identifying and mitigating threats caused by unknown vulnerabilities. It is applicable both before and after deployment and can be used to ensure the security and robustness of both in-house and third party software productions.

Save Resources

Most critical requirement for security testing is test coverage, and that ensures that most vulnerabilities still hiding in software are found proactively. The earlier vulnerabilities are found the easier and cheaper it is to fix them and the more thorough the fixes are. Moreover, if vulnerabilities are fixed, before the software is released, then there will not be any vulnerabilities for hackers to exploit.

No more Patch Rat Race

By finding and mitigating security issues proactively, you can avoid getting stuck in the endless rat race of deploying yet another patch, before attackers can create an exploit. By managing unknown vulnerabilities, you can anticipate upcoming patch releases and patch deployment no longer has to be a constant crisis management process. You can notify your customers of upcoming patch releases in beforehand and deploy all patches in one big push, a well planned security initiative. After all, downtime is always costly.

Extending Vulnerability Feeds

With the Defensics Traffic Capture Fuzzer you can generate tests from different types of vulnerability feeds and test system more thoroughly earlier. Vulnerability feed providers deliver security advisories and vulnerability information to their customers. Sometimes the actual exploit are provided as PCAP traffic recordings. In many cases, the vulnerability feed just contains general information about how to reproduce the vulnerability, and in those cases you can use Codenomicon Network Analyzer to capture and save the PCAP for later regression testing.

Build Defenses against Zero Day Attacks

Revealed attack surface can be narrowed with use of firewalls. And when blocking the interface is impossible, all millions of threats generated by Codenomicon Defensics come with extensive documentation to assist you in writing your tailored IDS rules. Defensics will automate the testing those defenses with extensive set of variations of all those real-life attack scenarios that it has generated, or that you have received from third party databases. Reproducing the attack scenarios with Defensics is very useful method of testing how well IDS/IPS systems and firewalls can detect and bloc both the original attack and variations of it.

Better Patches

By investigating security issues proactively, you gain more time and you can create better patches and also have time to test them. However, vendors usually create patches under considerable time pressure, and sometimes the quality of patches is not what it should be. With Codenomicon's Defensics fuzzers you can easily verify the quality of patches by testing them with variations of the original attack. Sometimes, even slight variations of the original attack can trigger new vulnerabilities.

5 How to Defend Your Systems

The Codenomicon Defensics model for Unknown Vulnerability Management consists of three phases: Analysis, Testing, Reporting and Mitigation. Unlike legacy vulnerability management processes, Fuzzing does not require a vulnerability assessment phase, because, in fuzzing, there are no false positives, and therefore all the found vulnerabilities are critical. In addition, the test suites automatically generate CWE (Common Weakness Enumeration) values for the found vulnerabilities. This industry standard method of evaluating vulnerabilities helps testers decide which vulnerabilities have the highest priority and need to be fixed first.



Figure 2: Unknown Vulnerability Management

Analyze

Use the Codenomicon Network Analyzer to map real network traffic and to determine what needs to be tested within your network. The Analyzer records traffic at multiple points in your network, thus it can capture the entire traffic in your network. It then automatically creates visualizations illustrating different aspects of the captured data. You can drill up and down from looking at high-level visualizations to inspecting the corresponding packet data, even in real time, and reveal hidden interfaces and possible exploits.

Test

Run multiple test suites simultaneously and discover both known and previously unknown vulnerabilities with unparalleled efficiency. Defensics provides intelligent specification based tools for over 200 protocols and file formats. Specification based tools contain all the possible protocol messages, and thus they can genuinely interoperate with the tested system exposing vulnerabilities even in deeper protocol layers. Unlike most XML Fuzzers, the state-aware Defensics XML Fuzzer not only tests XML parsers, but also all XML applications. The Traffic Capture Fuzzer creates tests from real traffic and can be used to test all protocols, and Generic File Format Fuzzer tests all file formats.

Report

Codonomicon test suites generate different reports for different audiences. Management reports provide a high-level overview of the test execution. Log files and spreadsheets help you to identify troublesome tests and to minimize false negatives. You can facilitate the technical analysis of individual tests by augmenting the already extensive test case documentation with PCAP traffic recordings. In addition, all important information is automatically collected into a Remediation Package, which you can send to third parties for automated reproduction.

Mitigate

Use the automatic features Defensics provides to quickly and easily reproduce vulnerabilities, perform regression testing and verify patches. The Codonomicon Defensics test suites automatically generate reports, which contain CWE values for the found vulnerabilities and direct links to the test suites that triggered the vulnerabilities. The CWE values help testers decide which vulnerabilities should be fixed first. Defensics also makes it easier to identify the test cases that triggered the vulnerability, to reproduce vulnerabilities and to verify patches. The test case documentation can be used to create tailored IDS rules to block possible zero-day attacks.

Collaborate

Manage tests carried out in multiple locations, process test results and coordinate the repair process in the Collab environment. In companies and organizations, the testing resources are often spread across geographical locations. The Codonomicon Collab enables users to remotely access the same system, thus they can execute the same tests, share results and other documentation, and reproduce the same vulnerabilities.

Services

Codonomicon also provides a number of security services ranging from creating custom tools to trial tests and coordinating the process of fixing the found vulnerabilities.

6 Conclusion

DEFENSICS test tools help enterprises secure their networks and applications from known and previously unknown protocol-level attacks. With the Codonomicon Network Analyzer, you can find those hidden interfaces, and with the Codonomicon DEFENSICS test tools, you can find and mitigate vulnerabilities in applications and systems, before the hackers have a chance to exploit them. However, Codonomicon's Unknown Vulnerability Management is not just about making systems more robust and secure to prevent exploits and liability issues, it is also about improving sales and company reputation by providing customers better quality services.