Report

Cyber risk report 2013

Executive summary

The latest edition of HP's annual Cyber Risk Report reveals a threat vista both stranger and more familiar than current news headlines would lead the reader to expect. It's a landscape where exotic zero-day attacks turn heads in the security community while unglamorous older vulnerabilities cause the real mayhem; where the software with the most reported vulnerabilities may be better off than software with fewer; and where a piece of software that boasts billions of users can still lead to a compromise of your corporate network.

Figure 1. Software application security

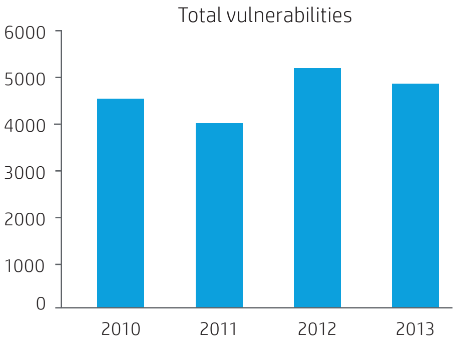
Software security

56%	Weakness revealing information about application, implementation, or user
31.5%	Prone to leaking system information through poor error handling

The HP 2013 Cyber Risk report, drawn from innovative work by HP Security Research (HPSR) in multiple focus areas, examines both the nature of the vulnerabilities that leave organizations unsafe (the organization's "attack surface") and how adversaries currently abuse those vulnerabilities. It challenges readers to think specifically about how their organization is apt to be attacked—and how best to allocate security funds to counter those threats. Among the key report findings:

- **Misconfigured systems give attackers a powerful boost:** Even well-written software can give attackers a foothold if not set up or maintained correctly after installation. When HP Fortify on Demand did in-depth analysis on a sampling of 2,200 applications, they found that 80 percent of the applications they saw were vulnerable to problems related to server misconfiguration, improper file settings, outdated versions of applications, or other post-implementation misfires. A clever attacker looks for those gaps; it's the responsibility of each organization to close them. The report points out that a diligent software auditing process and close attention to patching go a long way toward solving the problem.

Figure 2. Disclosed vulnerabilities measured by NVD, 2010–2013[1]



- **Number of new vulnerabilities holds steady; high-severity vulnerabilities on the decline:** The total number of publicly disclosed vulnerabilities remained at roughly the same levels seen in the previous three years, with the volume decreasing about 6 percent (figure 2) from last year. Meanwhile, high-severity vulnerabilities continued their multi-year decline in volume, reflecting vendors' use of newer security technologies such as sandboxing. Digging down and Cross-Frame Scripting attacks, which last year's report found pervasive, are still a notable problem today.
- **Internet Explorer and supervisory control and data acquisition (SCADA) provide the happiest hunting for researchers:** In 2013, HP Zero Day Initiative (ZDI) doubled its intake of vulnerabilities affecting the Microsoft® Internet Explorer browser. It also doubled the number of vulnerabilities it accepted related to SCADA infrastructure management software. But, the report notes that both Internet Explorer and SCADA are particularly tempting to researchers—IE because of its massive install base and SCADA for its ubiquity in critical industrial processes (as well as its role in 2010's Stuxnet saga). Researchers in a free market tend to investigate the software and platforms most likely to prove rewarding (financially, reputationally, and otherwise). The report cautions readers not to assume that the number of vulnerabilities reported in a package truly reflects its safety relative to similar software.
- **Don't believe the mobile malware hype:** Though reports of malware directed at mobile platforms (particularly Android) created significant news all year, an investigation by HP on data provided by ReversingLabs reveals that in 2013, mobile malware had yet to make significant inroads among the hundreds of thousands of applications available via Google™ Play.

  The research indicates that many public claims about rampant Android infection may stem from discrepancies in how industry observers judge the behavior and intent of mobile applications, especially ad-supported mobile applications. There's also still great variability in how the industry seeks, finds, and protects against problems on the Android platform. Though consumers and developers should continue to follow smart security practices when downloading mobile applications, the report notes that modern mobile operating systems have security baked in—and that mobile platforms are still doing better than their desktop counterparts.

[1] nvd.nist.gov/download.cfm

Figure 3. Mobile apps security

Mobile apps security

52%	Security issues were a result of insecure client-side operation
48%	Insecure server-side application code or code quality issues—unstable application behavior
74%	Unnecessary permissions

- **But don't get too comfortable:** As organizations scramble to meld their mobile and desktop workflows, HP Security Research took a hard look at how application developers build and adopt hybrid development strategies for mobile platforms. Their study found that the hybrid development frameworks available don't sufficiently address a number of issues already well known to desktop developers. The most pressing issue identified in the report is missing or weak encryption in native mobile applications, thus carrying potentially high risks for related hybrid mobile applications. HPSR found that nearly 46 percent of iOS and Android applications analyzed use encryption improperly.

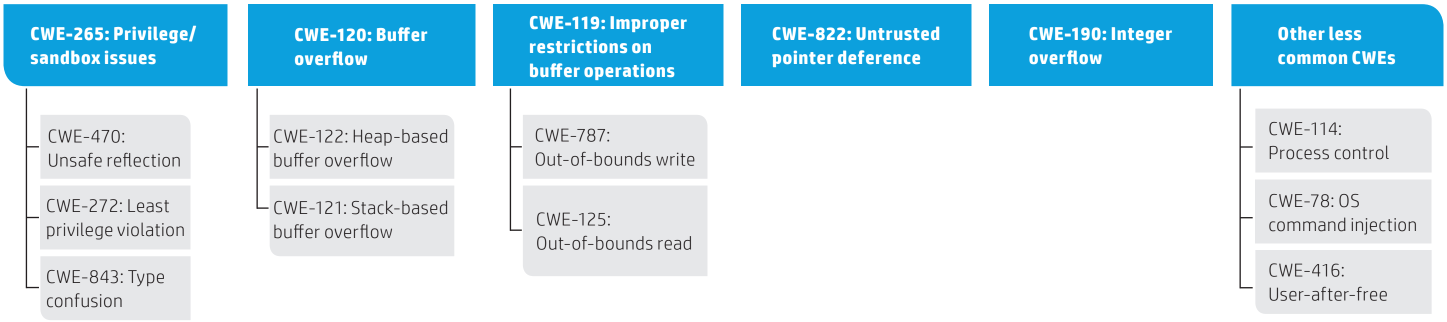
  Moreover, ZDI data indicates that plenty of vulnerabilities already known on traditional platforms can be equally effective on mobile devices using the same attack techniques, vectors, and targets. Worse, users tend to trust their handy mobile devices more than they trust their desktops, making certain techniques (social engineering attacks, for instance) far more effective. As the line between mobile and desktop usage blurs, and as users become more accustomed to having access to sensitive data on any platform they please, such issues will rise in importance. In the meantime, organization defenders face the difficult task of socializing best security practices among their people, while waiting for the development community to hold up its end.

- **Escalating attacks on Java may mean it's time to kick the habit:** Even though Microsoft products were the target of over half the vulnerabilities submitted to ZDI in 2013, Oracle's Java platform has drawn a great deal of criticism for insecurity, most notably when the US Department of Homeland Security urged users in January 2013 to uninstall the software. HP Security Research agrees that Java poses genuine risks but recognizes that many organizations require Java for mission-critical applications.

  A ZDI analysis of Java's actual attack surface indicates that Java's complex architecture of sub-components is susceptible to, literally, every common type of software vulnerability—but different sub-components are more prone to different types of attack. Increasingly in 2013, savvy adversaries mixed and matched, blending exploits against multiple vulnerabilities to form effective attacks. Researchers who successfully targeted Java at the Pwn2Own contest in March 2013 used four separate types of vulnerability to win. In addition, certain weaknesses are relatively easy for even moderately diligent researchers to use far and wide, allowing one exploit to compromise multiple iterations of Java without regard to the host operating system or application.

  The report recommends that organizations using Java make it a priority to apply Oracle's patches as soon as they become available. Analysis shows that many exploits are still in active use for months or years after the vulnerability they target is disclosed, and even after patches for that vulnerability are made available. Though the report stops short of recommending that organizations abandon Java, it does suggest that organizations evaluate their true need for it, uninstalling it from computers whose users don't require the technology for their work role.

Figure 4. Common weaknesses (CWE) in Oracle Java


CWE-265: Privilege/ sandbox issues
CWE-470: Unsafe reflection
CWE-272: Least privilege violation
CWE-843: Type confusion
CWE-120: Buffer overflow
CWE-122: Heap-based buffer overflow
CWE-121: Stack-based buffer overflow
CWE-119: Improper restrictions on buffer operations
CWE-787: Out-of-bounds write
CWE-125: Out-of-bounds read
CWE-822: Untrusted pointer deference
CWE-190: Integer overflow
Other less common CWEs
CWE-114: Process control
CWE-78: OS command injection
CWE-416: User-after-free

Resources

To download the full copy of the HP 2013 Cyber Risk Report, click here.

Real world attacks rely on patience as much as expertise

The report closes with a look at a March 2013 malware attack in South Korea in which banks and television networks in one of the world's most wired nations were kneecapped—not by a cutting-edge attack crafted by the world's greatest security professionals, but by relatively unsophisticated tools in the hands of patient, motivated, organized adversaries. The case study provides a look at how relatively well-known and well-understood techniques and tools can be combined to create mayhem—in the case of the South Korean attack, to maliciously destroy data and impede Internet access, or potentially to provide cover for the theft of intellectual property, financial information, or other sensitive data. In addition to traditional best security practices, the report provides guidance for further protecting organizations from this type of determined attack.

Conclusion

The HP 2013 Cyber Risk Report is a result of HP Security Research expertise and intelligence, the same intelligence that informs and guides the vision of HP Enterprise Security Products. What we've learned as an organization is that security is more than a product. It's about an integrated, systematic approach that includes both protective and reactive measures, and that has the same flexibility to share information that our adversaries employ in the real world. It's about repeated monitoring, testing, and building a process. It's about creating a platform that lets you truly manage your risk in a world where the cost and damages of breaches continue to rise in tandem with the complexity of security itself. And HP knows how to build that. The simple truth is that it takes an organization of HP's scale—one who has the experience, portfolio, and knowledge—to get this right. And in this world, you can no longer afford to be wrong. Not even once.

Learn more at
hp.com/go/sirm

Sign up for updates
hp.com/go/getupdated

4AA5-0920ENW, February 2014