HP Security Research Cyber Risk Report 2015

The annual Cyber Risk Report from HP Security Research provides organizations with a better understanding of the threat landscape and supplies resources that can aid in minimizing security risk. This year's report features perspectives drawn from advanced data analysis and takes a focused look at multiple technologies, including open source, mobile, and the Internet of Things.

Déjà Vu: Attackers Focusing on Older Vulnerabilities

8227
days from launch of first Windows version affected by **CVE-2014-4114** ("Sandworm") vuln to release of the patch - April 16, 1992 to October 14, 2014

59
combined maximum age, in years, of the code in the high-profile Heartbleed, Shellshock, and POODLE zero-days
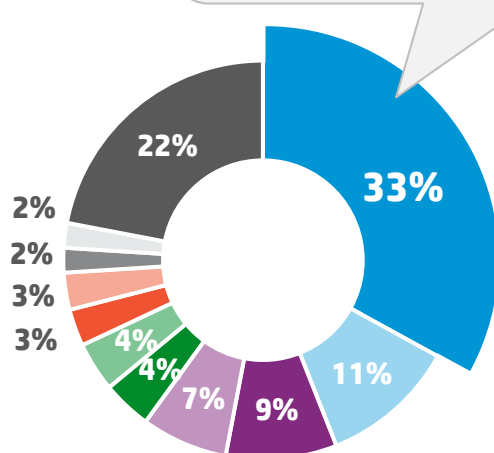
7 of the top 10 exploits used vulnerabilities that were discovered pre-2013
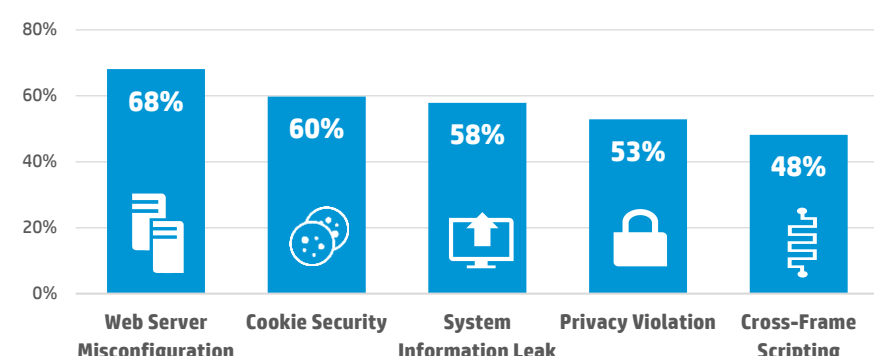
Top Exploits Discovered in 2014

- CVE-2010-2568 — 33%
- CVE-2010-0188 — 11%
- CVE-2013-2422 — 9%
- CVE-2012-1723 — 7%
- CVE-2012-0507 — 4%
- CVE-2012-0158 — 4%
- CVE-2012-2465 — 3%
- CVE-2012-4681 — 3%
- CVE-2013-2423 — 2%
- CVE-2009-3129 — 2%
- Others — 22%

33% of all exploit samples discovered in 2014 used an infection vector first detected in use in 2010, in Stuxnet
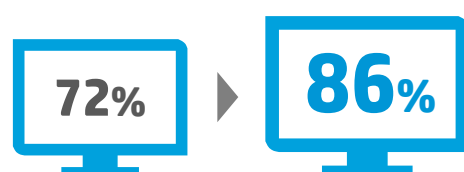
Server Misconfigurations Top Vulnerability List

- Web Server Misconfiguration — 68%
- Cookie Security — 60%
- System Information Leak — 58%
- Privacy Violation — 53%
- Cross-Frame Scripting — 48%

- Server misconfigurations were the most common category of vulnerabilities across all analyzed apps

2013 vs. **2014**

72% ▸ **86%**
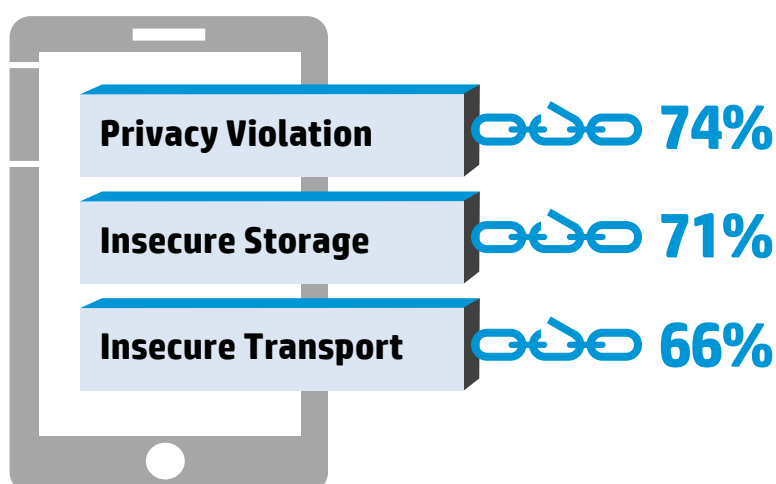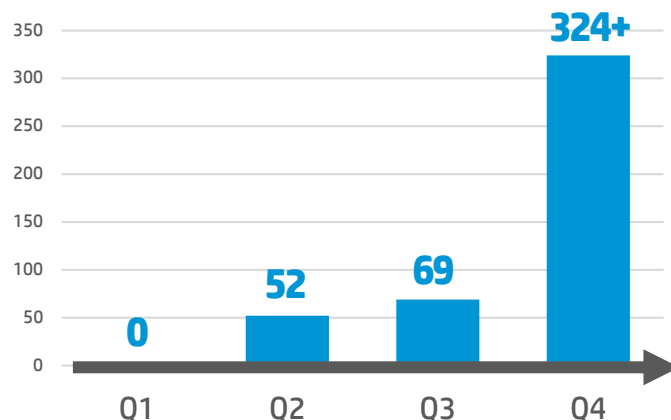
- Year over year change in % of web apps that exhibit one or more flaws in "Security Feature" development

Spotlight on Mobile

Top Mobile App Vulnerabilities

- Privacy Violation — **74%**
- Insecure Storage — **71%**
- Insecure Transport — **66%**

Number of Android ransomware samples detected in 2014, by quarter
(through November)

- Q1 — 0
- Q2 — 52
- Q3 — 69
- Q4 — 324+

Notable Numbers, Rankings, and Statistics

0
Major Oracle Java zero-days discovered in the wild in 2014

6
Pre-2014 Oracle Java vulnerabilities in the list of top ten 2014 exploit samples

On our minds:

> malware   [Search]

top keyword searched by security practitioners (even besting "Security")

#1
Rank of Microsoft as subject of ZDI disclosures in 2014

#11
Rank of most-exploited IE vulnerability in Top 50 CVEs list

#6
Rank of most-exploited MS Office vulnerability in Top 50 CVEs list

HP Zero Day Initiative

400+
Record-breaking number of high-severity vulnerabilities disclosed and remediated through the ZDI

US Canada Italy
Countries with highest submission rates to the ZDI since 2004

3000+
Independent researchers working with the ZDI to expose and remediate weaknesses
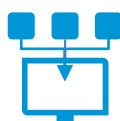
Recommendations

- Understand the changing threat landscape
- Develop and follow a patch strategy
- Conduct penetration testing and configuration verification
- Employ complementary technologies
- Share threat intelligence with the community

Learn More

Visit hp.com/go/cyberrisk to download the full report and access all Cyber Risk Report resources.

Brought to you by HP Security Research