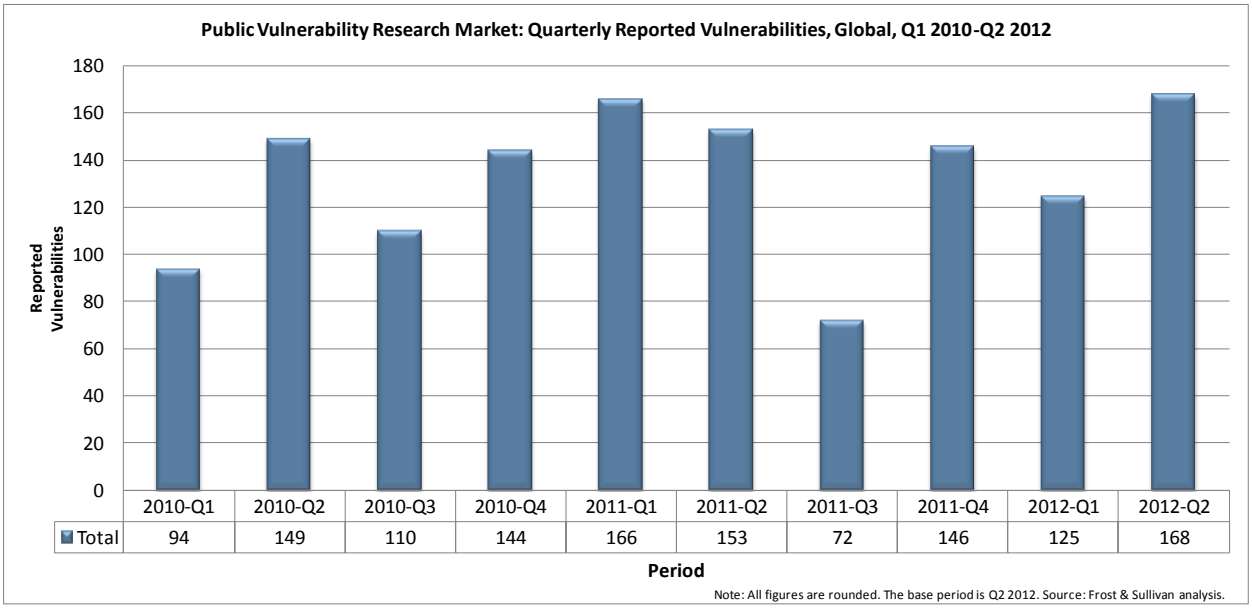
FROST & SULLIVAN

Analysis of the Global Vulnerability Research Market

Executive Summary

The necessity of vulnerability research is becoming increasingly evident as cyber attacks are orchestrated to breach networks and compromise applications. In order to stay ahead of the threat, security research labs, government entities, manufacturers, and individuals must work together to discover and report vulnerabilities. This collaborative approach enables vendors to develop and issue patches/updates to protect their applications and, most importantly, its users.

In Q2 2012, vulnerability research reporting increased 34.4 percent since Q1 2012. This sizable increase of reports can be attributed to security labs reporting that many vulnerabilities can take up to six months to be published. In doing so, this ensures manufactures of applications have ample time to issue a patch and provide its customers the proper steps to mediate the vulnerability.

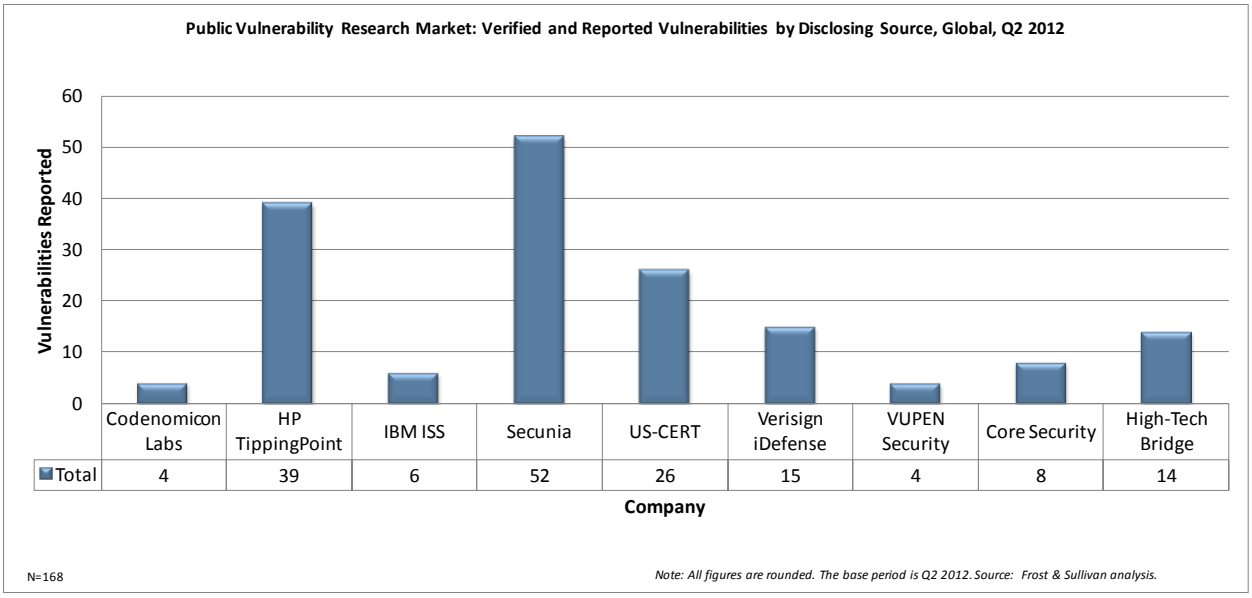


Frost & Sullivan research identified the top three applications attacked in Q2 2012 as Oracle Java Runtime Environment, Apple QuickTime, and Microsoft Windows. These applications

accounted for over 20 percent of the vulnerabilities disclosed in Q2. Cisco WebEx Player, Microsoft Internet Explorer, and Adobe Flash Player were also top targeted applications. As a result, media applications, business applications, software platforms, and web browsers were the top targets for vulnerability research and testing.

The top vulnerabilities in Q2 2012 were buffer errors; permission, privileges, and access control; and numeric errors. These vulnerabilities result in one or more negative effects on applications and networks such as remote code execution, denial-of-service, and/or file modifications.

Since 2006, Secunia has consistently been a top reporter in Frost & Sullivan's vulnerability research trackers. In Q2 2012, Secunia disclosed 52 verified vulnerabilities and 124 total vulnerabilities*, making Secunia the leader in vulnerability disclosure for the second quarter in a row. Secunia's emphasis on research in third-party applications has garnered the company much market success. Some of the vulnerabilities reported stemmed from Oracle Java Runtime Environment (14) and Adobe Illustrator (6).



With criminals building upon existing malware and customizing it to achieve their motives, it is critical that the security community responsibly shares vulnerability disclosures and invests in vulnerability research. Security vendors that identify new vulnerabilities through original research or contributor programs provide immeasurable value to their customers and to the security industry. Secunia's success in investing in their research activities and providing high-value services has lead the company to the top position in vulnerability disclosure during the first half of 2012..

* In *Analysis of the Vulnerability Research Market*, Frost & Sullivan distinguishes between verified and unverified vulnerabilities. A verified vulnerability must have an associated CVE number.