Analysis: Android has more vulnerabilities than Windows 10

March 10 2020, by Peter Grad

Credit: CC0 Public Domain

Although Windows 10 users are used to complaining about bugs and upgrades, they may be surprised to learn that Android and Linux have more vulnerabilities.

These and many more findings about the security of operating systems and [software programs](#) were posted last week by the privacy advocacy group thebestvpn.com. They analyzed 20 years of data collected by the National Institute of Standards and Technology's National Vulnerability Database.

The study examined vulnerabilities found in operating systems including Microsoft, Apple, Google, Mozilla and Linux, as well as in software programs such as Adobe Flash, Microsoft Office and Apple iTunes.

Among the more notable results: Over the past two decades, Debian Linux suffered 3,067 technical vulnerabilities, "rendering it the most vulnerable product," according to the analysis. The report notes that the Linux community of users is "very responsive" to reports of problems and that [vulnerability](#) issues are often resolved within days.

In the same time period, Windows 10, released in 2015, had 1,111 vulnerabilities.

In 2019, the most recent year surveyed, Android topped the list of problem-plagued systems, reporting 414 problems, 54 more than the open source Linux, with 360. Programming defects among third-party programs included on Android phones accounted for a portion of those vulnerabilities. Windows 10 recorded 357 bugs last year.

The report notes that in 1999, a total of 894 vulnerabilities were reported. Nearly 20 years later, in 2018, that number had soared to 16,566. Last year the number decreased, to 12,174.

On average, technical glitches are uncovered in just under 200 days and are contained in 69 days.

In discussing the types of security breaches that can impact millions of

desktop, laptop and mobile phone users, the report states that code execution in which a hacker gains access to execute arbitrary commands or code on a targeted device accounts for a quarter of all vulnerabilities. Nearly a fifth of security breaches involve cross-site scripting on web apps that allow attackers to activate code onto web pages viewed by others.

Other vulnerabilities include denial of service attacks, security bypass, unauthorized access to private data and memory corruption.

The report also assigned scores on a scale of 1 to 10 to software programs accumulating the most vulnerabilities over the years. Adobe Flash Player topped the list with a 9.4 score. Microsoft Office scored 9.1, Internet Explorer 8.6, iTunes 7.5, and watchOS, the least vulnerable of 15 programs analyzed, scored 7.4.

The thebstvpn.com is operated by privacy advocates who have been testing and writing about virtual private networks, VPNs, since 2015.

"There is cause for worry," the report notes in its introduction. "Our findings show that technology products housing your sensitive data have become increasingly vulnerable to bad actors over the past 20 years. Everything from your bank information to what you print out is susceptible, but that doesn't have to be acceptable."

Editors at thebestvpn.com, who have analyzed more than 70 virtual private networks and run hundreds of user reviews and comparison guides of various VPN programs, recommend setting up a private network as the best means "to keep your browsing history and data out of criminal hands."

  More information: thebestvpn.com/vulnerability-alerts/