This is one of the reasons why Linux is more secure than other operating system platforms

Although not the most commonly used operating system in the world, or as widely known as its competitors.

But it's probably not an exaggeration to say that Linux is currently a much more secure platform than Microsoft Windows and Apple macOS, at least according to a new report published by the Google Project Zero security organization.

However, Linux is highly appreciated by experts in terms of security, not because the operating system is inherently safe. The main reason lies in the enthusiasm and serious work of the developer community who maintain this platform, especially in the aspect of fixing reported vulnerabilities on the platform.

There have been quite a few reports of bugs and security holes in Linux documented. However, that does not mean that this operating system platform is not safe for everyday use. The latest research results from Project Zero show that Linux developers are doing the job of fixing security bugs faster than other platforms, to the surprise of even experts.

Project Zero's January 2019 to December 2021 annual statistics report shows that the average time it takes software vendors to release security patches is 52 days. However, it took only about 25 days for open source developers to fix a zero-day issue detected and reported by Project Zero - which is twice as fast as average. In addition, Linux developers also need less time to patch security flaws. Back in 2019, Linux programmers used to take around 1 month to fix a bug, now they do it within 2 weeks.

Do a few simple comparisons. Apple took about 69 days, Google took 44 days, and Mozilla fixed the bug in about 46 days. Windows is currently the world's most popular computer operating system, but it took Microsoft nearly three months to patch a reported security bug.

Deadline adherence and fix time 2019-2021, by bug report volume

Vendor	Total bugs	Fixed by day 90	Fixed during grace period	Exceeded deadline & grace period	Avg days to fix
Apple	84	73 (87%)	7 (8%)	4 (5%)	69
Microsoft	80	61 (76%)	15 (19%)	4 (5%)	83
Google	56	53 (95%)	2 (4%)	1 (2%)	44
Linux	25	24 (96%)	0 (0%)	1 (4%)	25
Adobe	19	15 (79%)	4 (21%)	0 (0%)	65
Mozilla	10	9 (90%)	1 (10%)	0 (0%)	46
Samsung	10	8 (80%)	2 (20%)	0 (0%)	72
Oracle	7	3 (43%)	0 (0%)	4 (57%)	109
Others*	55	48 (87%)	3 (5%)	4 (7%)	44

TipsMake

Zero-day vulnerabilities are security issues that were not known to software developers at the time they were discovered, or known but have not been patched. In general, these are all high-severity vulnerabilities that, if not fixed in time, can be exploited by hackers and deploy malicious activities causing great damage. Therefore, the shorter the break time, the more important it is for the overall security of the platform. In addition, the shorter the response time and patch release, the more likely the vulnerability is to receive the attention of service providers, thereby reducing risks for both users. In these respects, it can be said that Linux developers have been doing very well.

Google Project Zero is one of the most highly regarded security organizations in terms of expertise today. When a vulnerability is discovered, the team will give developers 90 days to fix security issues, before releasing all relevant information. The findings of Project Zero not only have important implications for Google's own products, but can also "save" many large organizations and businesses from the risk of a cybersecurity disaster.