Crossing the Digital Divide (v56)

"Patch Tuesday"

By Joseph Feigon for the Observer

Microsoft "Patch Tuesday" returned last week, sorry I couldn't give all the Windows 10 users a heads' up, it was a big one. Yes, I encourage, as does Microsoft, that you keep your PC up-to-date.

Software, for the most part, is developed, or written, by groups of engineers. Microsoft's Excel, or spreadsheet program, by recent estimates, is over 30 million lines of code. LibreOffice, an OpenSource alternative to Microsoft Office, contains over 12 million lines of code. Google's Chrome is roughly 5 million lines of code. On one hand, it might appear the OpenSource engineers are more efficient. On the other hand, navigating 100 lines of code is daunting, let alone a few million!

All that geeky comparative data aside, we know people make mistakes. Add disparate workgroups to the mix, and the known fact "we'll discover flaws in the field," software development is continual – discovered coding errors, discovered flaws in someone else's coding effort (most software talks to other software) and security vulnerabilities revealed through regressive testing and real-world experience.

Stay updated!

Here's a few notices from Microsoft about the March 2017 release:

Cumulative Security Update for Internet Explorer (4013073)
This security update resolves vulnerabilities in Internet Explorer. The most severe of the vulnerabilities could allow remote code execution if a user views a specially crafted webpage using Internet Explorer. An attacker who successfully exploited these vulnerabilities could gain the same user rights as the current user. If the current user is logged on with administrative user rights, an attacker who successfully exploited this vulnerability could take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

Security Update for Microsoft Office (4013241)
This security update resolves vulnerabilities in Microsoft Office. The most severe of the vulnerabilities could allow remote code execution if a user opens a specially crafted Microsoft Office file. An attacker who successfully exploited the vulnerabilities could run arbitrary code in the context of the current user. Customers whose accounts are configured to have fewer user rights on the system could be less impacted than those who operate with administrative user rights.

Security Update for Windows Kernel (4013081)
This security update resolves vulnerabilities in Microsoft Windows. The vulnerabilities could allow elevation of privilege if an attacker runs a specially crafted application.

Security Update for Adobe Flash Player (4014329)
This security update resolves vulnerabilities in Adobe Flash Player when installed on all supported editions of Windows 8.1, Windows Server 2012, Windows Server 2012 R2, Windows RT 8.1, Windows 10, and Windows Server 2016.

You can get all the details, and a far more extensive list here: https://technet.microsoft.com/en-us/library/security/ms17-mar.aspx

Control the things you can control.