

[TechNewsWorld](#) > [Security](#) | [Next Article in Security](#)

August 12, 2020 05:32:21 PM

Please note that this material is copyright protected. It is illegal to display or reproduce this article without permission for any commercial purpose, including use as marketing or public relations literature. To obtain reprints of this article for authorized use, please call a sales representative at (818) 461-9700 or visit <http://www.ectnews.com/about/reprints/>.

INDUSTRY ANALYSIS

Microsoft Code Leak Invokes Issues Beyond Security

By Jay Lyman

Feb 17, 2004 10:58 AM PT

▼ advertisement

[Webinar: Verifying Global Identities at Scale](#)

On Tues, Aug 25 at 10am PDT, learn about the challenges organizations face when trying to identify fraud, and how Ekata uses sophisticated data science and machine learning to create powerful and unique data insights to help with fraud risk assessments.

[Register Today!](#)

The recent disclosure of a security hole revealed through the leak of Microsoft Windows 2000 and NT source code is raising several issues that the software giant will have to face as a result of the breach. Analysts are indicating the leak could have a profound effect not only on the security of Microsoft's software, but also on the company's worldwide reputation.



In addition to the source-code leak, an alert from SecurityTracker indicates a vulnerability and related exploit in Internet Explorer version 5 was discovered over the weekend. The vulnerability itself, which does not affect Internet Explorer 6, does not stand out as a significant new weakness because Internet Explorer has been pummeled in the last several months by several vulnerabilities, exploits and attacks.

However, the source-code leak and the new IE vulnerability, taken together, mark the beginning of what is expected to be a painful period for Microsoft.

[Forrester](#) research director Michael Rasmussen told TechNewsWorld that the limited source-code leaks, although incomplete and for earlier versions of Microsoft's operating systems, have

implications for other OSs, including Windows XP. "I would say that on other Microsoft OSs that yes, there is exposure," Rasmussen said, "because there's legacy code. Microsoft doesn't write every OS from scratch."

Advantage Attackers

In posting the vulnerability and exploit based on the leaked source code -- which was being volleyed among Internet sites, FTP sites, peer-to-peer (P2P) networks and elsewhere -- a researcher outlined a relatively simple integer overflow attack that could take advantage of a discovered vulnerability in the source code.

Security experts such as iDefense malicious code director Ken Dunham, who told TechNewsWorld that attackers were touting the leak as a leg up for them against Microsoft, said the increase in publicly disclosed vulnerabilities likely will hit fast.

"As a result of this breach, the likelihood of new attacks, especially zero-day attacks [that have no warning or patch], has significantly increased for Windows NT and Windows 2000 platforms," Dunham said. "Anyone with significant assets at risk will need to apply due diligence like never before and embrace predictive and rapid response solutions to help mitigate new threats that will emerge in 2004."

Other Systems at Risk

While the leak was limited to incomplete portions of the Windows 2000 and NT source code, [Gartner](#) research vice president Richard Stiennon told TechNewsWorld that the software code is more than enough to enable researchers and attackers to punch holes in other Windows systems.

Forrester's Rasmussen, who expected to see an uptick in vulnerabilities that are already emerging more quickly than corresponding patches from Microsoft, said the revealed source code shows Microsoft is struggling with security.

"It's sad that it was released, and it's sad it was written so [badly] from a security standpoint," he said, adding that the breach will affect almost all operating systems from Microsoft.


"I expect all of the Windows operating systems to be exposed under the hood," Rasmussen said.

Reputation and Rivals

Dunham said the code also might be used by those who hate Microsoft -- already a vocal group that has targeted the software company's site and services -- to further tarnish Microsoft's reputation and image.

"Many online users were very excited about the software leak, in some cases saying, 'Death to Microsoft; long live open source,'" Dunham said. "The distribution of Microsoft's source code is just one blow to the software giant. The integrity of these files, outside of Microsoft, cannot be verified. As a result, some users might add various hard-coded back-door components or other elements in an attempt to skew facts and defame Microsoft."

Rasmussen, who indicated there is an advantage to the inherent availability of open-source software, said Microsoft also might be hurt by competitors that use the widely available, leaked Windows source code.

"I would like to think most companies are going to be above board and hold up to intellectual property laws," Rasmussen said. "But there could be some advantage for companies that want to borrow, bake and steal [from the leaked code]." 

▼ advertisement

Ekata Webinar | Tuesday, August 25th | 10am PDT

Join us for our live webinar where Stacy Chen, Senior Product Marketing Manager at Ekata will discuss some of the challenges businesses are facing when it comes to identity verification and how Ekata can help with fraud risk assessments. [Register Today!](#)

 [Get Permission to License or Reproduce this Article](#)

 [Reprints](#)  [More by Jay Lyman](#)

Reader Comments

 [Be the first to comment!](#)