

# Microsoft aims barrage of fixes at Stuxnet and more

October 12 2010

---



Microsoft on Tuesday released a record high number of software patches aimed at countering computer threats including a Stuxnet "worm" attacking industrial networks.

Microsoft on Tuesday released a record high number of software patches aimed at countering computer threats including a Stuxnet "worm" attacking industrial networks.

The 49 fixes released by [Microsoft](#) were ranked in importance from "critical" to "moderate" and addressed vulnerabilities in an array of Microsoft programs used in personal computers.

"Users should apply these patches ASAP," said Trend Micro threat researcher Ivan Macalintal. "It should be a top priority."

The unprecedented number of fixes promised to make installing the

patches a chore for technology workers managing business networks.

"The release is humongous; a record breaker," Macalintal said. "I think it is going to be a headache, especially for enterprise (business systems)."

Microsoft bulletin MS10-073 indicated a patch for a vulnerability that Stuxnet "currently leverages."

Stuxnet targets control systems made by German industrial giant Siemens commonly used to manage water supplies, oil rigs, [power plants](#) and other industrial facilities.

Stuxnet has been dubbed the world's "first cyber superweapon" by experts, and has wreaked havoc on computerized industrial equipment in Iran.

Microsoft previously patched two of the four vulnerabilities that Stuxnet took advantage of in Windows-based computer networks. The patch released on Tuesday is intended to close a third door to the [malicious software](#).

The vulnerability exploited by Stuxnet allowed an elevation of control privileges for the program once it was in a Windows-based network, according to Kaspersky Lab Americas senior anti-virus researcher Roel Schouwenberg.

"As such I think the real life impact on the spread of Stuxnet will be rather limited," Schouwenberg said.

"Machines are either going to be already patched for the remotely exploitable vulnerabilities which would introduce Stuxnet onto the system or they're not going to have any of the Stuxnet related patches installed."

Analysts say [Stuxnet](#) may have been designed to target Iran's nuclear facilities, especially the Russian-built first atomic power plant in the southern city of Bushehr.

(c) 2010 AFP

Citation: Microsoft aims barrage of fixes at Stuxnet and more (2010, October 12) retrieved 10 May 2024 from <https://phys.org/news/2010-10-microsoft-aims-barrage-stuxnet.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.