



Australian Government

Attorney-General's Department



AUSTRALIA'S NATIONAL
COMPUTER EMERGENCY RESPONSE TEAM

CERT Australia Industry News

Out of Band patch released for Windows Shell vulnerability.

Microsoft has released an out of band patch [1] to correct a publically disclosed vulnerability in the Windows Shell.

Technical Details

The vulnerability, which if successfully exploited, resulted in the execution of arbitrary code due to the way Windows would parse shortcut files. Exploiting this vulnerability would require a user to browse to a directory where the malicious shortcut file would be saved. The malicious file could be transported via infected USB devices, network shares, drive-by downloads from a website, or by malicious email attachments. The extent of the damage the exploit would cause is limited to the user privileges of the account the malware ran on.

Business Impact

This vulnerability was originally seen to be used in targeted attacks against SCADA systems through the use of a new malware family named Stuxnet [2]. This vulnerability has since also been used in the distribution of a number of malware families including key logger Zeus [3]. In the business environment this patch would prevent unauthorised code execution via the original vulnerability. In cases where the vulnerability was exploited, attackers could take complete control of machines which could then be used to perform further attacks against the enterprise. Users should check that anti-virus is working and up-to-date as if this vulnerability has already been exploited and systems compromised, this patch may not necessarily rectify the infection.

Further Reading

[1] <http://www.microsoft.com/technet/security/bulletin/ms10-046.msp>

[2] <http://www.microsoft.com/security/portal/Threat/Encyclopedia/Entry.aspx?Name=Worm%3aWin32%2fStuxnet.A>

[3] <http://www.f-secure.com/weblog/archives/00001996.html>

This document remains the property of the Australian Government. The information contained in this document is for the use of the intended recipient only and may contain confidential or privileged information. If this document has been received in error, that error does not constitute a waiver of any confidentiality, privilege or copyright in respect of this document or the information it contains. This document and the information contained herein cannot be disclosed, disseminated or reproduced in any manner whatsoever without prior written permission from the Assistant Secretary, E-Security Policy and Coordination, Attorney-General's Department, 3 - 5 National Circuit, Barton ACT 2600.

The material and information in this document is general information only and is not intended to be advice. The material and information is not adapted to any particular person's circumstances and therefore cannot be relied upon to be of assistance in any particular case. You should base any action you take exclusively on your own methodologies, assessments and judgement, after seeking specific advice from such relevant experts and advisers as you consider necessary or desirable. To the extent permitted by law, the Australian Government has no liability to you in respect of damage that you might suffer that is directly or indirectly related to this document, no matter how arising (including as a result of negligence).