



**Centre for Critical Infrastructure Protection
Threat Information Product (TIP)**

**Out-Of-Band Microsoft Update
Windows Shortcut Handling Vulnerability**

Serial Number: CCIP-TIP_UA6A100802-01

Date: Monday 2 August 2010

This information must be handled in accordance with the above Traffic Light Protocol (TLP)¹ handling caveat.

Summary:

CCIP commenced monitoring of a vulnerability affecting Windows .LNK files (commonly referred to as shortcuts) on 16th July 2010. On 17th July (Local Time), Microsoft released a [security advisory](#) on the issue. The issue also affects .PIF files.

CCIP have received reports of attacks in New Zealand attempting to exploit this vulnerability. However, previous CCIP alerting was not deemed appropriate as mitigations or solutions were deemed impractical.

Microsoft has now scheduled the release of an [out-of-band security bulletin](#) for Tuesday, 3rd August 2010 (local Time). According to Microsoft, the bulletin will address this security vulnerability in all supported editions of Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, Windows 7, and Windows Server 2008 R2.

Degree of Credibility:

Highly Credible

Vulnerability confirmed by Vendor.

Impact Criticality:

Highly Critical

The vulnerability exists because Windows incorrectly parses shortcuts in such a way that malicious code may be executed when the icon of

¹ For a definition of the TLP please contact CCIP or see the following link:

<http://www.ccip.govt.nz/incidents/tlp.html>



a specially crafted shortcut is displayed. This vulnerability can be exploited locally through a malicious USB drive, or remotely via network shares and WebDAV. An exploit can also be included in specific document types that support embedded shortcuts.

Level of Verification:

Confirmed

Confirmed by Vendor and attacks reported to CCIP.

Availability of Exploit:

Confirmed

Proof of concept code published and widely available. Numerous attacks (including attacks in New Zealand) have been reported.

Solution:

As with all security updates, CCIP recommends that organizations review, test and apply this update as soon as possible after its release.

Discussion:

CCIP would welcome any feed back or comments on this alert. If you should be targeted by such an attack please report it to CCIP. As and when CCIP becomes aware of any further relevant information we will update this alert.

Links:

<http://www.microsoft.com/technet/security/Bulletin/MS10-aug.msp>

<http://www.microsoft.com/technet/security/advisory/2286198.msp>