Security News

2011-28013 Microsoft Internet Explorer Time Element Memory Corruption Vulnerability

1. Affected Version

Microsoft Internet Explorer 6
Microsoft Internet Explorer 7
Microsoft Internet Explorer 8

2. Description

A remote code execution vulnerability exists in the way that Internet Explorer accesses an object that has not been correctly initialized or has been deleted. The vulnerability may corrupt memory in such a way that an attacker could execute arbitrary code in the context of the logged-on user.

3. Vulnerability Analysis

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

```
<HTML XMLNS:t="urn:schemas-microsoft-com:time">
<?IMPORT namespace="t" implementation="#default#time2〃>
<body>
<div id="x" contenteditable="true"
style='width:0;height:0;visibility:hidden'>
MMu9090u9090u10EBu4B5BuC933uB966u03F3u3480uE20BuFAE2u05EBuEBE8uFF[...snip...]
XXu1d16u77c2u1104u77c1u44c3u77c2u2000u0000u1000u0000u0040u0000uc0[...snip...]
OOu0d20u0d0du5ed5u77c1u0d20u0d0du0d20u0d0du5ed5u77c1u0d20u0d0du0d[...snip...]
TTu0d0fu0d0eKKJJu0d0du0d0dLL1043416UU
<t:TRANSITIONFILTER></t:TRANSITIONFILTER>
<script type="text/javascript">
```

Table 1: The partial proof-of-concept code

The vulnerability is caused due to the error when accessing an object that has been incorrectly initialized or has been deleted. A remote attacker can exploit this vulnerability by enticing a target user to open a maliciously crafted Web page.

Successful exploitation may allow remote attackers to gain the same user rights as the logged-on user. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights.

4. Recommendation

1. AegisLab IDP signature database can prevent this attack since 12/07/2011.
2. Apply the appropriate patch for your system, as listed in Microsoft Security Bulletin MS11-050.

5. Reference

1. Microsoft Security Bulletin MS11-050 (Critical)
2. CVE-2011-1255