securing your web finjan Vital Security

MCRC Notification

Zero Day Attacks in the wild

This notification lists currently known Zero-Day attacks already seen in the wild. Finjan's Vital Security detects and blocks these attacks proactively, keeping our users safe.

1. WMI Object Broker Control (WmiScriptUtils.dll)

Description: A Vulnerability discovered in an ActiveX control in Visual Studio 2005 on Windows. This vulnerability could lead to Remote Code Execution by attacker on Victim's machine. The ActiveX control is the WMI Object Broker control, which is part of WmiScriptUtils.dll. The Microsoft WMI Object Broker ActiveX control bypasses the ActiveX security model.

Publish date: 01-Nov-2006
Severity: Extremely Critical
Vulnerability status: Un-patched by the vendor
Vital Security status: Protects against this vulnerability
References:
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-4704
http://www.kb.cert.org/vuls/id/854856

2. Microsoft Internet Explorer COM Object Instantiation Daxctle.OCX Heap Buffer Overflow Vulnerability

Description: Memory corruption vulnerability exists in Microsoft's daxctle.ocx ActiveX which can lead to remote code execution on fully patched machine.

Publish date: 14-Sep-2006
Severity: Extremely Critical
Vulnerability status: Un-patched by the vendor
Vital Security status: Protects against this vulnerability
References:
http://secunia.com/advisories/21910/
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-4777

3. ADODB.Connection ActiveX control

Description: The ADODB.Connection ActiveX control object can allow a denial of service (DoS) (Internet Explorer crash).

Publish date: 24-Oct-2006
Severity: Low
Vulnerability status: Un-patched by the vendor
Vital Security status: Protects against this vulnerability
References:
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-5559