June 14, 2011, 4:16PM

Microsoft Ships 16 Fixes in June's Patch Tuesday

by Brian Donohue

Microsoft patched nine critical vulnerabilities and seven important vulnerabilities, pushing out a total of 16 patches in the June edition of Patch Tuesday. One of the bugs patched was used to compromise Internet Explorer during the Pwn2Own contest this year.

Four of the critical vulnerabilities specifically affect Windows and could allow for remote code execution if unpatched. The first affects Windows Object Linking and Embedding Automation and could be exploited if an attacker convinced users to visit a Web site containing a specifically crafted Windows Metafile (WMF) image. The second occurs in Windows Kernel-Mode Drivers, and could allow remote code execution if a user visited a network share containing a specially crafted OpenType font (OTF). The third, and perhaps the most severe, is in the Distributed File System (DFS). This bug could allow an attacker to execute arbitrary code and take complete control of an affected system after sending a specially crafted DFS response to a client-initiated DFS request. The fourth vulnerability is in the SMB client, and to exploit it, an attacker must convince the user to initiate an SMB connection to a specially crafted SMB server.

Two more of the critical vulnerabilities take place in Internet Explorer. One is a cumulative security update that addresses 11 privately reported vulnerabilities, the most severe of which could allow an attacker to gain user privileges if that user views a specifically crafted Web page using Internet Explorer. The second resolves a privately reported vulnerability in the Microsoft implementation of Vector Markup Language (VML) that could be exploited in the same way to allow remote code execution.

Editor's Pick

Week in Security: Year-end E-Card Drama, Foreign Spies

There are two with critical bugs that affect the .NET framework. The first of them also addresses a vulnerability in Microsoft Silverlight. If unpatched, it could allow remote code execution on a client system if a user views a specially crafted Web page using a Web browser that can run XAML Browser Applications (XBAPs) or Silverlight applications. It could also be exploited on a server system running IIS, if that server allows processing ASP.NET

and Sandboxes - Not So Safe After All?

Microsoft Ships 12 Bulletins in February's Patch Tuesday

Microsoft Readies 'Critical' Windows, IE Patches

Threatpost Newsletter Sign-up

pages and an attacker succeeds in uploading a specially crafted ASP.NET page to that server and then executes the page. It could also be used by Windows .NET applications to bypass Code Access Security (CAS) restrictions. The second bulletin strictly affects the .NET framework and could be exploited in the same way.

The last of the vulnerabilities is in the Microsoft Forefront Threat Management Gateway (TMG) and resolves a privately reported vulnerability. It could allow for remote code execution if an attacker leveraged a client computer to make specific requests on a system where the TMG firewall client is used.

For more information on these patches and the complete list of bulletins, check out Microsoft's TechNet blog, where you will also find a webcast hosted by Microsoft tomorrow to address customer concerns regarding these bulletins.

Comments

Post new comment

Your name:

Anonymous

E-mail:

The content of this field is kept private and will not be shown publicly.

Comment: *

Path: