

TopResponse Threat Advisory

Release Date: October 21, 2011.

Purpose: The Corero TopResponse team is issuing an advisory, which provides information needed to block known attacks targeting the Microsoft Forefront Poisoned Cup of Code Remote Code Execution Vulnerability (MS11-079,CVE-2011-1969).

Corero Products: Top Layer IPS 5500 E-Series and later.

Vulnerable Infrastructure: Microsoft Forefront Unified Access Gateway 2010, Microsoft Forefront Unified Access Gateway 2010 Update 1, Microsoft Forefront Unified Access Gateway 2010 Update 2, and Microsoft Forefront Unified Access Gateway 2010 SP1.

Alert Type: Critical Vulnerability

Risk Assessment: Critical

Threat Impact: Remotely exploitable vulnerability that could allow an attacker to control vulnerable systems

Advisory Impact: Prevention

Summary: Microsoft Forefront Unified Access Gateway (UAG) utilizes a signed Java applet. There is a vulnerability in the way the signed Java applet is used that can result in remote code execution on any user browser that supports Java. The reported vulnerability could allow an attacker to execute arbitrary code on the users systems in the context of the logged-on user by enticing the user to open a specially crafted web site.

Recommended Action: Corero recommends the following actions:

Download and apply Protection Pack 2011-10-19-01 (or later) to put this new protection into place. This will put into place protection for the Microsoft Forefront Poisoned Cup of Code Remote Code Execution Vulnerability that will be applied to the “Recommended Client Protection” IPS Rule Set.

In order to take advantage of the protection provided in this Protection Pack, make sure the IPS rule tln-106391 is enabled in the IPS Rule Set used to inspect traffic to your Microsoft Forefront Unified Access Gateway infrastructure.

References: Use the following sources for additional information:

Additional Information	Location
------------------------	----------

Corero Support	http://www.corero.com/support
Microsoft Advisory	http://www.microsoft.com/technet/security/bulletin/ms11-079.msp

Relevant IPS 5500 Rules: tln-106391.

Relevant TopResponse Protection Pack(s): 2011-10-19-01.