

"Faci quod potui, faciant meliora potents!"

Calculator is the arbitrary (shell)code for MS08-078 example module.

HTML	XML Island	DSO 1.0	DSO 3.0	DSO 3.0
	<div>Launch1</div>	<div>Launch</div>	<div>Launch</div>	<div>Launch</div>
<DIV>	<div>Launch</div>	<div>Launch</div>	<div>Launch</div>	<div>Launch</div>
<MARQUEE>	<div>Launch</div>	<div>Launch</div>	<div>Launch</div>	<div>Launch</div>
<LABEL>	<div>Launch2</div>	<div>Launch</div>	<div>Launch4</div>	<div>Launch</div>
<LEGEND>	<div>Launch</div>	<div>Launch</div>	<div>Launch</div>	<div>Launch</div>
<DIV> 	<div>Launch3</div>	<div>Launch</div>	<div>Launch</div>	<div>Launch</div>

[Click on "Launch" for the correspondent HTML Element and DSO.]




Permutation Oriented Programming

©2004-2011 Nelson Brito. All rights reserved worldwide.

Please, find below some explanations about:

1. How the MS08-078 demonstration applying Permutation Oriented Programming works;
2. How you might perform the tests based on each example; and
3. How you might interpret the results of each example.

<div>1</div>	<p>The exploitation elements are:</p> <ol style="list-style-type: none">1. XML Data Island:<ol style="list-style-type: none">a. HTML <XML> Element is present.2. XML Data Source Object Reference:<ol style="list-style-type: none">a. HTML <XML> Element is present and holds the DSO;b. CDATA (Unparsed Character Data) is present; andc. HTML Element is present.3. Data Consumer:<ol style="list-style-type: none">a. HTML Element is present and repeated. <p><i>Note: It is in compliance with the CVE description for the vulnerability MS08-078, so any IDS/IPS should detect and prevent this attack exploitation alternative. For further details, please, refer to: CVE-2008-4844.</i></p>
--------------	---

	<p>The exploitation elements are:</p> <ol style="list-style-type: none"> XML Data Island: <ol style="list-style-type: none"> HTML <XML> Element is present. XML Data Source Object Reference: <ol style="list-style-type: none"> HTML <XML> Element is present and holds the DSO; CDATA (Unparsed Character Data) is present; and HTML Element is present. Data Consumer: <ol style="list-style-type: none"> HTML <DIV>, <MARQUEE>, <LABEL> and <LEGEND> Elements are present and repeated. <p><i>Note: They ARE NOT in compliance with the CVE description for the vulnerability MS08-078, so some IDS/IPS should FAIL to detect and prevent these attack exploitation alternatives. For further details, please, refer to: CVE-2008-4844.</i></p>
	<p>The exploitation elements are:</p> <ol style="list-style-type: none"> XML Data Island: <ol style="list-style-type: none"> HTML <XML> Element is present. XML Data Source Object Reference: <ol style="list-style-type: none"> HTML <XML> Element is present and holds the DSO; CDATA (Unparsed Character Data) is present; and HTML Element is present. Data Consumer: <ol style="list-style-type: none"> HTML and <DIV> Elements are present and mixed. <p><i>Note: It IS NOT in compliance with the CVE description for the vulnerability MS08-078, so some IDS/IPS should FAIL to detect and prevent this attack exploitation alternative. For further details, please, refer to: CVE-2008-4844.</i></p>
	<p>The exploitation elements are:</p> <ol style="list-style-type: none"> XML Data Source Object Reference: <ol style="list-style-type: none"> HTML <OBJECT> Element is present and holds the DSO, using different class identifications: <ul style="list-style-type: none"> 550DDA30-0541-11D2-9CA9-0060B0EC3D39 F5078F39-C551-11D3-89B9-0000F81FE221 F6D90F14-9C73-11D3-B32E-00C04F990BB4 CDATA (Unparsed Character Data) is present; and HTML Element is present. Data Consumer: <ol style="list-style-type: none"> Please, refer to the previous explanations (1, 2 and 3) for each HTML Element alternative. <p><i>Note: These alternatives bypass "Disable XML Island functionality" workaround issued by Microsoft, and they ARE NOT in compliance with the CVE description for the vulnerability MS08-078, so some IDS/IPS should FAIL to detect and prevent these attack exploitation alternatives. For further details, please, refer to: CVE-2008-4844.</i></p>

The following scenario and environment is strictly recommended to perform demonstrations and/or tests:

1. Extract the contents of “MS08-078_XML_Island_Bypass.zip” into your WEB Server root directory.
2. Map your WEB Server to use “index.html”.
3. Place your IDS/IPS at the network segment you will use to access the WEB Server.
4. Browse the WEB Server and choose one of the options.

