What is Microsoft EMET and why should I care?
What is Microsoft EMET and why should I care?

<table>
<thead>
<tr>
<th>1. REPORT DATE</th>
<th>2. REPORT TYPE</th>
<th>3. DATES COVERED</th>
</tr>
</thead>
<tbody>
<tr>
<td>22 OCT 2014</td>
<td>N/A</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>4. TITLE AND SUBTITLE</th>
</tr>
</thead>
<tbody>
<tr>
<td>What is Microsoft EMET and why should I care?</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>6. AUTHOR(S)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dormann /William</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Software Engineering Institute Carnegie Mellon University Pittsburgh, PA 15213</td>
</tr>
</tbody>
</table>

Approved for public release, distribution unlimited.
ROP Mitigations

EMET 4.0 provides application-specific ROP mitigations

- LoadLibrary
- MemProt
- Caller
- SimExecFlow
- StackPivot
LoadLibrary

Extra checking when loading a library.

- e.g. don’t allow loading from a UNC path
Memprot

Check memory protection functions like VirtualProtect to make sure they are not doing things like marking stack as executable.
Caller

Before critical API functions called, disassemble backwards to verify that target function is called.

- Don’t allow return into function (“Return” of ROP)
SimExecFlow

Forward execution simulation to verify normal program execution flow.
StackPivot

When entering a critical function, make sure that stack pointer is within bounds of the stack.
EMET 5.0 New Features

EMET 5.0 includes additional exploit mitigations

- Attack Surface Reduction
- EAF+
- Deep Hooks Enabled
Attack Surface Reduction

Reducing attack surface critical to prevention of exploitation.

Examples:

• Only allow Java in Intranet IE zone.
• Don’t allow Flash in Microsoft Word
EAF

Export Address Filtering

To perform useful functionality, shellcode usually needs to call exported functions.

e.g. `kernel32!WinExec()`

EAF blocks access to Export Address Table (EAT) based on calling address.
EAF+

Export Address Filtering +

- Added KERNELBASE export protection
- Integrity checks on stack registers and stack limits
- Prevent memory operations for export tables when they originate from suspicious modules.
EAF+ In Action

Deep hooks

Protection of high-level functions applied towards lower-level function as well.

Microsoft has been working with vendors to make sure to ensure deep hooks compatibility.
Use EMET to stay safe

The only way to safely run applications on Windows is to use EMET!

- Minimize risk of delayed patching
- Protect against known vulnerabilities
- Protect against 0day vulnerabilities
- Protect against future vulnerabilities
EMET Recommend Configuration

System Status

- DEP Application Opt Out
- SEHOP Application Opt Out
- ASLR Always On*

Import Popular Software.xml

Add every application you care about
For More Information

Visit CERT® web sites:
http://www.cert.org
http://www.cert.org/vuls/discovery/
http://www.cert.org/blogs/certcc/

Contact Presenter
Will Dormann
wd@cert.org
(412) 268-8922

Contact CERT:
Software Engineering Institute
Carnegie Mellon University
4500 Fifth Avenue
Pittsburgh PA 15213-3890