Everyday software vulnerabilities and their exploitation threaten the user information system and computing experience. Often, common applications like word processing, media players, browser and its extensions are used to reap the rich benefits for personal and professional productivity, becomes the target of these threats. A significant problem lies in the way these vulnerabilities are exploited, which requires no user interaction, as they gets downloaded and executed simply by visiting a malicious website or opening a malicious downloaded document. A normal user wouldn’t have any clue of what components of the browser or the running application is being exploited either for installation of malware for vicious purpose or for propagation of malware to other systems.

User and Enterprise rarely patch these third party products due to numerous factors like lack of availability of tools, half cooked or broken patching process, lack of security governance and organizational culture. The frequency of zero day attacks is on raise for the client side applications according to various vulnerability intelligence companies worldwide including IBM X-Force Threat reports. According to SANS report “The Top Cyber Security risks” the un-patched client-side software is on the top priority number one from the rest of the risks. It is interesting and frustrating to note that some of the vendors haven’t patched the zero day vulnerabilities reported two years ago according to SANS report.

It is a well known fact that signature based Anti malware detection and removals technology products are losing the war as these technologies can’t keep up with the wide variety of malware and its variants being produced on daily basis. The only solution which holds promise is to address these vulnerabilities at the very heart of the operating systems to counter various attacks exploiting the underlying operating system mechanisms. Microsoft recently released “Enhanced Mitigation Experience Toolkit” (referred to as EMET) version 2.0.0.3 in November 2010 for its fleet of client and server operating systems including Windows XP, Windows VISTA, Windows 7, Windows Server 2003 and 2008. At the time of release, EMET was not supported by Microsoft. For the enterprise environments EMET’s MSI format can be deployed either manually or by existing software deployment delivery mechanism/tool.

The success of EMET really depends on the acceptability of this tool in the user community and its wider deployment. The demand for its support forced Microsoft to support the EMET. Also, much needed feature for the success of this technology in enterprise market segment would be manageability of EMET by the group policy, without which chances of EMET deployment in enterprise market are dull. EMET will be another layer of defense in the defense in depth strategy in near future to mitigate or in worse cases delay exploits being successful on the target systems.

EMET mitigation tool looks really nifty due to the controls offered at the very root of the exploits taking on the Microsoft platform like stack overflow and address randomization. EMET offers mitigation
techniques such as dynamic Data Execution Prevention (DEP is enabled by default on IE8), Structured Exception Handler Overwrite Protection (SEHOP), Heap Spray Allocation, Null Page Allocation, Export Address Allocation Table Access Filtering and Mandatory Address Space Layout Randomization. EMET kit offer granularity up to the single process. For more details of this mitigation tool and how does it work, please refer to EMET user guide (see the reference list at the end of this article). It will be prudent to enrol browsers, Acrobat Reader, flash players in the EMET to prevent exploitation of this application while surfing web sites.

Supported systems

EMET 2.0 supports the following operating systems and service pack levels:

Client Operating Systems:
• Windows XP service packs 3 and above
• Windows Vista service pack 1 and above
• Windows 7 all service packs

Server Operation Systems:
• Windows Server 2003 service pack 1 and above
• Windows Server 2008 all service packs
• Windows Server 2008 R2 all service packs

Configuration of EMET

EMET can be configured using the graphical interface or by the commands.

Listing 1 - Main EMET configuration windows with the options per process and system wide configuration.
After you install EMET, you will need to specify how much protection to provide. Click on the **configure system** button as shown in listing 1. This will open a new window as shown in listing 2.

![System Configuration Window](image1.png)

**Listing 2- System configuration**

Next click on the configure application button and screen in listing 3 will come. In this, you can add application by clicking add button, this would protect the added applications. Finally, reboot your device for changes to take place.

![Application Configuration Window](image2.png)

**Listing 3- Application configuration**

EMET is really a good control initiative at the fundamental causes of vulnerabilities in Microsoft products and promises another defense in depth layer for protecting the information systems. As user acceptance and demand for EMET raises, we will see further development of these tools for its integration via group policy. It will be good to see this tool being fully supported and managed via group policy in near future. Needless to say, this mitigation needs to be tested for deployment in the
production environment as it may break existing application compatibilities therefore production implementation will require extensive testing before it can be deployed. Again, EMET could serve as another layer in the defence depth strategy.

References


About the author

Naveen Sharma CISA, CISSP, CISM and SANS-GCIH. He works for an Insurance company in Sydney, Australia. His interest lies in Malware analysis, Operating system assurance techniques and Network forensics.