Microsoft Office – Memory corruption vulnerability

CVE[1] number : CVE-2015-2510[1]
SEVERITY SCORE : 9.3/10

Score Legend:

- Low risk < 4.0. Loss is likely to have only a limited adverse effect.
- Medium risk 4.0-6.9. Loss is likely to have a serious adverse effect.
- High risk 7.0-10.0. Loss is likely to have a catastrophic adverse effect.

Vulnerability Release Date: 9/8/2015
Vulnerability Analysis Date: 9/9/2015

Description: Buffer overflow in the Adobe Type Manager Library allows remote attackers to execute arbitrary code via a crafted OpenType font, aka "Graphics Component Buffer Overflow Vulnerability".
Visibility: publicly disclosed – not in the wild
Impact: Remotely exploitable - Allows unauthorized disclosure of information - Allows unauthorized modification - Denial of service

Summary

Microsoft Excel could allow a remote attacker to execute arbitrary code on the system, caused by improperly accessing an object in memory. By persuading a victim to open a specially-crafted document, an attacker could exploit this vulnerability to corrupt memory and execute arbitrary code on the system with the privileges of the victim.

A proof-of-concept code has been publicly disclosed [2]. This increases the risk of successful exploitation of this vulnerability.

Applies to:

- Microsoft Office 2007 SP3;
- Microsoft Office 2010 SP2.

Security Monitoring Analysis

Even if no specific information is available regarding this vulnerability, the attack pattern to exploit Microsoft Office vulnerability goes through a series of well-known steps.

Microsoft Office memory corruption vulnerabilities permit the attacker to execute a piece of code that is already present in the reader memory. The attacker delivers the actual malicious code and then the vulnerability is exploited by a technique called ‘heap-spray’ which consists of filling the reader memory with the malicious code. The allocated memory needs to be large enough for the memory layout to be predicted and the vulnerability exploitation to be reliable.

From a user point of view, a heap-spray can be noticed because the reader becomes unresponsive, its memory grows dramatically and its CPU usage reaches 100%.

Stormshield Endpoint Security automatically detects this technique when the setting ‘Protection against memory overflow’ is set to ‘Low’ or above.

[1] CVE is a dictionary of publicly known information security vulnerabilities and exposures

In the event the attacker is able to execute the malicious code by delivering it without being blocked by the heap-spray protection of Stormshield Endpoint Security, the attack plan follows a well-known two-step sequence.

Execution: first step

Since the malicious code is always located in a non-executable memory area, the operating system would terminate the offending application while attempting to execute this code. To bypass this protection, the aim of the first step is to make some memory area executable and it will contain the remaining of the malicious code. This task is performed using a technique called ROP (Return Oriented Programming) to execute pieces of code borrowed from legitimate existing code.

Stormshield Endpoint Security detects this technique using the RCP (Ret-Lib-C Protection), monitoring sensitive functions used in typical malicious code. This protection is turned on when ‘Protection against memory overflow’ is set to ‘Low’ or above.

Execution: second step

The second step of the malicious code contains the effective payload. The main objective of this step is to install the malware on the system. To be able to perform this task, the malicious code needs to have access to services of the operating system (to write a file on the disk, to download some data from the Internet …). These services are retrieved from the kernel32 dynamic library that is loaded in all processes. The technique used to retrieve this module consists in browsing the list of modules loaded for the current process. This technique is well known and widely used because it is compatible with all Windows operating systems.

Stormshield Endpoint Security detects this technique using the HPP (Honey Pot Protection) by adding a fake kernel32 module in processes. This protection is turned on when ‘Protection against memory overflow’ is set to ‘Low’ or above.

Recommendation

Enable the ‘Protection against memory overflow’ feature in Stormshield Endpoint Security

In order to block typical attack techniques used in this class of vulnerabilities, it is recommended to set ‘Protection against memory overflow’ to ‘Low’ or above.

Solutions

Run all software as a non-privileged user with minimal access rights

To reduce the impact of latent vulnerabilities, run all processes with the minimum of privileges required for each functionality. In particular, avoid using accounts belonging to administrators' groups.

Do not accept or execute files from untrusted or unknown sources.

To reduce the likelihood of successful attacks, never handle or open files from unknown sources.

References

[1]	CVE Details	http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-2510
[2]	Public disclosure	https://code.google.com/p/google-security-research/issues/detail?id=469

Revision

9/10/2015: Initial Release

9/17/2015: Public disclosure