COMPUTER SECURITY BULLETIN

Risk/Impact Rating: SERIOUS

< MS Office Memory Corruption Vulnerability >

CSB17-006

Description:

Microsoft Office is prone to a remote memory-corruption vulnerability. An attacker can leverage this issue to execute arbitrary code in the context of the currently logged-in user. Failed exploit attempts will likely result in denial of service conditions.

Technologies Affected

- Microsoft Office 2007 SP3
- Microsoft Office 2010 (32-bit edition) SP2
- Microsoft Office 2010 (64-bit edition) SP2
- Microsoft Office 2016 for Mac
- Microsoft Office for Mac 2011
- Microsoft Word Viewer

Recommendations:

- Run all software as a nonprivileged user with minimal access rights, to reduce the impact of latent vulnerabilities;
- Deploy network intrusion detection systems to monitor network traffic for malicious activity;
- Do not accept or execute files from untrusted or unknown sources;
- Do not follow links provided by unknown or untrusted sources; and
- Implement multiple redundant layers of security. This tactic may complicate exploits of memory-corruption vulnerabilities.

References:

https://www.symantec.com/security_response/vulnerability.jsp?bid=95287
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7298