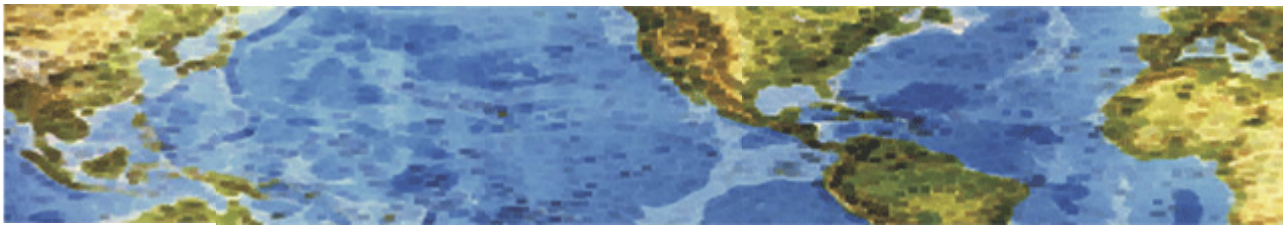
HALL ASSOCIATES



Risk-Based Decision Making Commentary
8 October 2013 Newsletter

Vulnerabilities in Microsoft Word Could Allow Remote Code Execution

Multiple vulnerabilities have been discovered in Microsoft Word that could result in remote code execution. Exploitation of these vulnerabilities may occur **if a user opens a specially crafted Word file** using Word in Microsoft Office 2003, Word in Microsoft Office 2007 or Microsoft Office Compatibility Pack SP3. Successful exploitation of these vulnerabilities could result in the **attacker gaining the same rights as the logged on user.** Depending on the privileges associated with the user, an attacker could then install programs, view, change, or delete data, or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights.

RISK:

Government:

- For Large and medium government entities: **High**
- For Small government entities: **High**

Businesses:

- Large and medium business entities: **High**
- Small business entities: **High**

Home users: High

RECOMMENDATIONS:

The following actions should be taken:

- Apply appropriate patches provided by Microsoft to vulnerable systems immediately after appropriate testing.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- View emails in plain text.
- Remind users not to open e-mail attachments from unknown users or suspicious e-mails from trusted sources.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.

https://technet.microsoft.com/en-us/security/bulletin/ms13-086

HALL ASSOCIATES

Cumulative Security Update for Internet Explorer

Multiple vulnerabilities have been discovered in Microsoft's web browser, Internet Explorer, which could allow an attacker **to take complete control of an affected system**. The systems affected are Internet Explorer 6, Internet Explorer 7, Internet Explorer 8, Internet Explorer 9, Internet Explorer 10 and Internet Explorer 11. Successful exploitation of these vulnerabilities could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

RISK:

Government:

- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:

- Large and medium business entities: **High**
- Small business entities: **High**

Home users: High

RECOMMENDATIONS:

The following actions should be taken:

- Apply appropriate patches provided by Microsoft to vulnerable systems immediately after appropriate testing.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Inform and educate users regarding the threats posed by hypertext links contained in emails or attachments especially from un-trusted sources.

REFERENCE:

https://technet.microsoft.com/en-us/security/bulletin/ms13-080