

*The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.*

**DATE(S) ISSUED:**

2/8/2011

**SUBJECT:**

Vulnerability in Microsoft PowerPoint Could Allow Remote Code Execution

**Overview:**

A vulnerability has been discovered in Microsoft PowerPoint, a program used for creating presentations. This vulnerability can be exploited by opening a specially crafted PowerPoint file received as an email attachment, or by visiting a web site that is hosting a specially crafted PowerPoint file. Successful exploitation could allow an attacker to gain 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.

**Please note that there is no patch available for this vulnerability.**

**Systems Affected:**

- Microsoft PowerPoint 2007

**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**

**Description:**

A vulnerability has been discovered in Microsoft PowerPoint which could allow an attacker to take complete control of an affected system. The vulnerability occurs when the application parses external objects in an 'Office Art' container. Successful exploitation of the vulnerability 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.

**Please note there is currently no patch available for this vulnerability.**

**Recommendations:**

The following actions should be taken:

- Apply appropriate patches provided by Microsoft to vulnerable systems as soon as they become available.
- 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.
- Remind users not to open email attachments from unknown or un-trusted sources.

**References:**

**Security Focus:**

- <http://www.securityfocus.com/bid/46228/>

**Zero Day Initiative:**

- <http://www.zerodayinitiative.com/advisories/ZDI-11-044/>