



**State of Alaska Cyber Security &  
Critical Infrastructure  
Cyber Advisory**

**December 9, 2008**

*The following cyber advisory was issued by the State of Alaska and was 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.*

**STATE OF ALASKA ADVISORY NUMBER:**

2008-027

**DATE(S) ISSUED:**

12/9/2008

**SUBJECT:**

Vulnerabilities in Microsoft GDI Could Allow Remote Code Execution

**OVERVIEW:**

Two vulnerabilities have been discovered in the Microsoft Graphics Device Interface (GDI). Microsoft Windows Graphic Device Interface (GDI) enables various applications to access devices which render images, such as desktop displays and printers, for the user. **GDI is installed by default on all Microsoft Windows operating systems.** These vulnerabilities can be exploited if a user views a malicious web page; views **or previews** an email message; or opens an email attachment containing a specially crafted image file designed to exploit one of the vulnerabilities. Successful exploitation will result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, the attacker could then install programs; view, change, or delete data; or create new accounts with full privileges.

**SYSTEMS AFFECTED:**

- Windows 2000 Service Pack 4
- Windows XP Service Pack 2 & 3
- Windows XP Professional x64 Service Pack 1 & 2
- Windows Server 2003 Service Pack 1
- Windows Server 2003 Service Pack 2
- Windows Server 2003 x64 Edition
- Windows Server 2003 x64 Edition Service Pack 2
- Windows Server 2003 with SP1 for Itanium-based Systems
- Windows Server 2003 with SP2 for Itanium-based Systems
- Windows Vista
- Windows Vista Service Pack 1
- Windows Vista x64 Edition
- Windows Vista x64 Edition Service Pack 1
- Windows Server 2008 for 32-bit Systems
- Windows Server 2008 for x64-based Systems

- Windows Server 2008 for Itanium-based Systems

**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:**

Microsoft Windows Graphic Device Interface (GDI) fails to properly handle Windows Metafile (WMF). Microsoft Windows Graphic Device Interface (GDI) enables various applications to access devices that render images, such as desktop displays and printers, for the user. **GDI is installed by default on all Microsoft Windows operating systems.**

All of the vulnerabilities mentioned in this advisory can be exploited if a user views a malicious web page; views **or previews** an email message; or opens an email attachment, such as a Microsoft Word document, that contains a specially crafted image file designed to exploit one of the vulnerabilities.

Once the user has opened the malicious WMF file a buffer overflow occurs because of the way the graphics device interface handles the malformed header of the attacker's WMF image. Successful exploitation will result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, the attacker could then install programs; view, change, or delete data; or create new accounts with full privileges.

**RECOMMENDATIONS:**

We recommend the following actions 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.
- Do not visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Read all e-mail messages in plain text.
- Turn off the preview pane on Microsoft Outlook.
- Do not open email attachments from unknown or un-trusted sources.
- Filter all incoming Windows format Metafile (WMF) content at email gateways and proxy servers. Note that WMF images are not typically used on web sites or to send images via email therefore blocking them should have little business impact.
- Update all custom software that uses GDI libraries.

**REFERENCES:**

**Microsoft**

<http://www.microsoft.com/technet/security/bulletin/MS08-071.msp>

**Security Focus**

<http://www.securityfocus.com/bid/32634>

<http://www.securityfocus.com/bid/32637>

**CVE**

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-3465>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-2249>