



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

October 14, 2009

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.

ADVISORY NUMBER:

SA2009-058

DATE(S) ISSUED:

10/14/2009

SUBJECT:

Multiple Vulnerabilities in GDI+ Could Allow Remote Code Execution (MS09-062)

OVERVIEW:

Multiple 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.

Please note: GDI+ is installed by default on all Microsoft Windows operating systems.

This vulnerability can be exploited if a user views a malicious web page; views or previews a malicious 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
- Windows XP
- Windows Server 2003
- Windows Vista
- Windows Server 2008
- Microsoft Visual Studio 2008
- Microsoft Visual Studio 2005
- Microsoft Visual Studio .NET 2003
- Microsoft Visual FoxPro
- Microsoft Visio 2002
- Microsoft SQL Server 2005

- Microsoft SQL Server 2000
- Microsoft Report Viewer 2008
- Microsoft Report Viewer 2005
- Microsoft Office XP
- Microsoft Office 2003
- Microsoft Office 2007
- Microsoft Project 2002
- Microsoft Platform SDK Redistributable: GDI+
- Microsoft Internet Explorer 6.0
- Microsoft Groove 2007
- Microsoft Forefront Client Security
- Microsoft Expression Web

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:

Multiple 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.**

WMF Integer Overflow Vulnerability

A remote code execution vulnerability exists in the way that GDI+ allocates buffer size when handling WMF image files.

PNG Heap and Integer Overflow Vulnerabilities

Two remote code execution vulnerabilities exists in the way that GDI+ allocates memory while opening specially crafted PNG image files.

TIFF Buffer Overflow and Memory Corruption Vulnerabilities

Two remote code execution vulnerabilities exists in the way that GDI+ allocates memory when opening specially crafted TIFF files.

.NET API Vulnerability

A remote code execution vulnerability exists in GDI+ that can allow a malicious Microsoft .NET application to gain unmanaged code execution privileges.. Microsoft .NET applications that are not malicious are not at risk for being compromised because of this vulnerability.

Memory Corruption Vulnerability

A remote code execution vulnerability exists in Microsoft Office that allows remote code execution if a user opens a specially crafted Office file that contains a malformed object.

Office BMP Integer Overflow Vulnerability

A remote code execution vulnerability exists in Microsoft Office that allows remote code execution if a user opens a specially crafted e-mail or opens an Office Document containing malformed BMP images.

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 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.

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.

REFERENCES:

Microsoft:

<http://www.microsoft.com/technet/security/Bulletin/MS09-062.msp>

<http://blogs.technet.com/srd/archive/2009/10/12/new-attack-surface-reduction-feature-in-gdi.aspx>

Security Focus:

<http://www.securityfocus.com/bid/36645>

<http://www.securityfocus.com/bid/36646>

<http://www.securityfocus.com/bid/36647>

<http://www.securityfocus.com/bid/36648>

<http://www.securityfocus.com/bid/36649>

<http://www.securityfocus.com/bid/36650>

<http://www.securityfocus.com/bid/36651>

CVE:

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2500>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2501>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2502>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2503>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3126>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2528>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2518>