



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

December 7, 2011

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:

SA2011-065

DATE(S) ISSUED:

12/13/2011

SUBJECT:

Vulnerability in Windows Kernel-Mode Drivers Could Allow Remote Code Execution (MS11-087)

OVERVIEW:

A vulnerability has been discovered in Microsoft Windows Kernel-Mode Driver. Exploitation of this vulnerability could result in the execution of arbitrary code with administrative privileges resulting in full control of the affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full system rights.

SYSTEMS AFFECTED:

- Microsoft Windows XP
- Microsoft Vista
- Microsoft Windows 7
- Microsoft Windows Server 2003
- Microsoft Windows Server 2008

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 identified in Microsoft Windows Kernel-Mode driver (win32.sys) that could allow for remote code execution. The "win32.sys" kernel-mode device driver provides various functions such as the window manager, collection of user input, and screen output. A remote code execution vulnerability exists in implementations of Microsoft Windows in which the kernel mode driver does not perform proper validation when writing TrueType fonts into a buffer.

UNCLASSIFIED

This vulnerability has been used to drop the Duqu malware by embedding a malformed font inside an Office Word document. An attacker could take advantage of this issue by getting a user to open a specially crafted file containing malformed TrueType fonts via a website, email, or by hosting the file on a network share. Successful exploitation will result in an attacker gaining the ability to install programs; view, change, or delete data; or create new accounts with full system rights.

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.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Apply the principle of Least Privilege to all services.

REFERENCES:

Microsoft:

<http://technet.microsoft.com/en-us/security/bulletin/ms11-087>

<http://blogs.technet.com/b/srd/archive/2011/12/13/more-information-on-ms11-087.aspx>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3402>

SecurityFocus:

<http://www.securityfocus.com/bid/50462>

Non-legitimate websites claiming to have the “hot” gift of the season when most legitimate retailers are sold out. The non-legitimate websites will tempt the victim to order from them when they actually do not have the item and will steal their personal information and charge their credit card².

PREVENTATIVE STRATEGIES

(U) The following preventative strategies are intended to help our public and private partners proactively look for emails attempting to deceive users into ‘clicking the link’ or opening attachments to seemingly real websites regarding holidays season ‘deals’. The following represents some best practices to follow but is not an exhaustive list:

NEVER click on links in emails. If you do think the email is legitimate, whether from a third party retailer or primary retailer, go to the site and log on directly. Whatever notification or service offering was referenced in the email, if valid, will be available via regular log on.

NEVER open the attachments. Typically, retailers will not send emails with attachments. If there is any doubt, contact the retailer directly and ask whether the email with the attachment was sent from them.

Do NOT give out personal information over the phone or in an email unless completely sure. Social engineering is a process of deceiving individuals into providing personal information to seemingly trusted agents who turn out to be malicious actors. If contacted over the phone by someone claiming to be a retailer or collection agency, do not give out your personal information. Ask them to provide you their name and a call-back number. Just because they may have some of your information does not mean they are legitimate! Again, be careful when providing any information over the phone. For further information regarding holiday scams, visit: http://www.us-cert.gov/current/index.html#holiday_season_phishing_scams_and

POINTS OF CONTACT

(U) While the U.S. Government does not endorse a particular solution, identifying vendors with experience managing cyber incidents may reduce the time it takes to mitigate damage and restore service or operations if compromised.

(U) Any cyber intrusion, including data breaches involving a monetary loss or financial nexus, can be reported to any of the FBI’s 56 Field Offices. For FBI field office contact information, please consult your local telephone directory or see the FBI’s contact information web page:

<http://www.fbi.gov/contactus.htm>

(U) US-CERT (www.us-cert.gov) offers a wide variety of technical and non-technical information to make use of both before and after an incident. A variety of documents with information regarding defensive measures to combat a computer network attack are available at:

<http://www.us-cert.gov/nav/t01/>

(U) Many organizations can suffer financial loss as a result of a cyber attack and may wish to pursue criminal or civil charges against the intruder. For legal advice, we recommend that you consult with your legal counsel and law enforcement. Data breaches involving a monetary loss or financial nexus such as a compromise to your credit or debit accounts, or personal information can also be reported to the U.S. Secret Service for criminal investigation. For more information contact your local Secret Service Field Office for assistance.

http://www.secretservice.gov/field_offices.shtml

(U) Non-U.S. entities may need to discuss malicious cyber activity with their local law enforcement agency to determine the appropriate steps that should be taken with regard to pursuing an investigation.

ENDNOTES:

1. *'Tis the Season to Get Hacked: Don't Become a Holiday Cybercrime Victim*, socialmediatoday.com - <http://socialmediatoday.com/jan-legnitto/395737/tis-season-get-hacked-don-t-become-holiday-cybercrime-victim>
2. *12 Scams of the Holidays: Do Not Let Cybercriminals Steal Your Holiday Spirit*, blogs.mcafee.com - <http://blogs.mcafee.com/consumer/12-scams-of-the-holidays-do-not-let-cybercriminals-steal-your-holiday-spirit>