

[VulnWatch] iDefense Security Advisory 02.22.07: VeriSign ConfigChk ActiveX Control Buffer Overflow Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/VulnWatch/2007-02/msg00021.html>

- *From:* iDefense Labs <labs-no-reply@xxxxxxxxxxxx>
 - *Date:* Thu, 22 Feb 2007 17:27:05 -0500
-

VeriSign ConfigChk ActiveX Control Buffer Overflow Vulnerability

iDefense Security Advisory 02.22.07

<http://labs.iddefense.com/intelligence/vulnerabilities/>

Feb 22, 2007

I. BACKGROUND

The ConfigChk ActiveX Control is part of VeriSign Inc.'s MPKI, Secure Messaging for Microsoft Exchange and Go Secure! products. It looks for the Microsoft Enhanced Cryptographic Provider in order to support 1024-bit cryptography.

II. DESCRIPTION

Remote exploitation of a buffer overflow vulnerability in VeriSign Inc.'s ConfigChk ActiveX Control could allow an attacker to execute arbitrary code within the security context of the victim.

The ActiveX control in question, identified by CLSID 08F04139-8DFC-11D2-80E9-006008B066EE, is marked as being safe for scripting.

The vulnerability specifically exists when processing lengthy parameters passed to the VerCompare() method. If either of the two parameters passed to this method are longer than 28 bytes, stack memory corruption will occur. This amounts to a trivially exploitable stack-based buffer overflow.

III. ANALYSIS

Successful exploitation of this vulnerability would allow a remote attacker to execute arbitrary code within the context of the victim.

In order to exploit this vulnerability, an attacker would need to persuade the victim into viewing a malicious web site. This is usually accomplished

by getting the victim into clicking a link in a form of electronic communication such as e-mail or instant messaging.

IV. DETECTION

iDefense has confirmed the existence of this vulnerability within version 2.0.0.2 of VeriSign Inc's VSCnfChk.dll. All versions are suspected to be vulnerable.

V. WORKAROUND

Setting the kill-bit for this control will prevent exploitation of this vulnerability through Internet Explorer.

VI. VENDOR RESPONSE

VeriSign has addressed this vulnerability by releasing a patch which corrects the security issues found in the affected .dll file.

VII. CVE INFORMATION

A Mitre Corp. Common Vulnerabilities and Exposures (CVE) number has not been assigned yet.

VIII. DISCLOSURE TIMELINE

12/22/2006 Initial vendor notification
12/20/2006 Initial vendor response
02/22/2007 Coordinated public disclosure

IX. CREDIT

This vulnerability was discovered by David D. Rude II (iDefense).

Get paid for vulnerability research
<http://labs.idefense.com/methodology/vulnerability/vcp.php>

Free tools, research and upcoming events
<http://labs.idefense.com/>

X. LEGAL NOTICES

Copyright © 2007 iDefense, Inc.

Permission is granted for the redistribution of this alert electronically. It may not be edited in any way without the express written consent of iDefense. If you wish to reprint the whole or any part of this alert in any other medium other than electronically, please e-mail customerservice@xxxxxxxxxxxxx for permission.

Disclaimer: The information in the advisory is believed to be accurate at

the time of publishing based on currently available information. Use of the information constitutes acceptance for use in an AS IS condition. There are no warranties with regard to this information. Neither the author nor the publisher accepts any liability for any direct, indirect, or consequential loss or damage arising from use of, or reliance on, this information.