

[VulnWatch] iDefense Security Advisory 04.04.07: ESRI ArcSDE Buffer Overflow Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/VulnWatch/2007-04/msg00012.html>

- *From:* iDefense Labs <labs-no-reply@xxxxxxxxxxxxx>
 - *Date:* Wed, 04 Apr 2007 21:37:56 -0400
-

ESRI ArcSDE Buffer Overflow Vulnerability

iDefense Security Advisory 04.04.07

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

Apr 04, 2007

I. BACKGROUND

Environmental Systems Research Institute (ESRI) ArcSDE is a multi-user database server that has been bundled with ArcGIS to provide access to Geographic Information Systems (GIS). More information is available at ESRI's web site located at the following URL.

<http://www.esri.com/software/arcgis/arcscde/index.html>

II. DESCRIPTION

Remote exploitation of a buffer overflow vulnerability within Environmental Systems Research Institute (ESRI) Inc.'s ArcSDE service allows attackers to execute arbitrary code in the context of the running service.

This vulnerability appears to exist in the handling of requests containing overly long string parameters. By supplying a specially crafted request, the ArcSDE server will overflow a buffer and overwrite execution control information stored on the stack.

III. ANALYSIS

Exploitation allows attackers to execute arbitrary code with the privileges of the running service.

No authentication is required to exploit this vulnerability. The attacker only needs the ability to converse with the server via the TCP port on which it is listening. By default the server listens on port 5151.

IV. DETECTION

An iDefense contributor reported that version 9.2 is vulnerability to this attack. ESRI confirmed the vulnerability. All prior versions are suspected to be vulnerable.

V. WORKAROUND

Employing firewalls to limit access to the affected service can help prevent potential exploitation of this vulnerability.

VI. VENDOR RESPONSE

ESRI has identified this issue as NIM007075 and corrected the vulnerability by releasing ArcGIS 9.2 Service Pack 2. Additionally, ESRI released the "Three Tiered Connection Security Patch" to address the problem in older versions. For more information see ESRI's notifications at the following URLs.

<http://support.esri.com/index.cfm?fa=downloads.patchesServicePacks.viewPatch&PID=66&MetaID=1259>
<http://support.esri.com/index.cfm?fa=downloads.patchesServicePacks.viewPatch&PID=19&MetaID=1262>
<http://support.esri.com/index.cfm?fa=downloads.patchesServicePacks.viewPatch&PID=19&MetaID=1261>
<http://support.esri.com/index.cfm?fa=downloads.patchesServicePacks.viewPatch&PID=19&MetaID=1260>

VII. CVE INFORMATION

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

VIII. DISCLOSURE `TIMELINE

02/13/2007 Initial vendor notification
02/15/2007 Initial vendor response
04/04/2007 Coordinated public disclosure

IX. CREDIT

The discoverer of this vulnerability wishes to remain anonymous.

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

[VulnWatch] iDefense Security Advisory 04.04.07: ESRI ArcSDE Buffer Overflow Vulnerability

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.