

[VulnWatch] [SecurityOffice] Enceladus Server Suite v3.9 Buffer Overflow Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/VulnWatch/2002-12/0001.html>

From: Tamer Sahin (ts@securityoffice.net)

Date: 12/09/02

Date: Mon, 9 Dec 2002 20:32:06 +0200
From: Tamer Sahin <ts@securityoffice.net>
To: vulnwatch@vulnwatch.org

-----BEGIN PGP SIGNED MESSAGE-----

Hash: MD5

--[Enceladus Server Suite v3.9 Buffer Overflow Vulnerability]--

--[Type

Buffer Overflow

--[Release Date

December 09, 2002

--[Product / Vendor

Enceladus Server Suite is an Internet/Intranet lightweight Web and FTP Server for Windows, provides secure file sharing on any network. Perfect for Broadband, Cable Modem, Small business and Personal Use. You don't have to be an expert to setup file sharing or run your own web site and FTP Server. This Server Suite is One of the Easiest To Install and Operate.

<http://www.mollensoft.com>

--[Summary

Enceladus Server Suite is vulnerable to a buffer overflow condition. An attacker may supply a long sequence of characters as an argument to "CD" command.

If the length of the supplied string exceeds the size of its input buffer, the excess data will overwrite other variables on the stack and the stack frame itself. It is possible for a malicious user to craft a request that will result in code execution on the vulnerable system.

--[Tested

VulnWatch: [VulnWatch] [SecurityOffice] Enceladus Server Suite v3.9 Buffer Overflow Vulnerability

@@
@@
@@@@@@@@@@@@

421 Service not available, remote server has closed connection.

===== SNIP =====

--[Disclaimer

<http://www.securityoffice.net> is not responsible for the misuse or illegal use of any of the information and/or the software listed on this security advisory.

--[Author

Tamer Sahin
ts@securityoffice.net
<http://www.securityoffice.net>

All our advisories can be viewed at <http://www.securityoffice.net/articles/>

Please send suggestions, updates, and comments to feedback@securityoffice.net

(c) 2002 SecurityOffice

This Security Advisory may be reproduced and distributed, provided that this Security Advisory is not modified in any way and is attributed to SecurityOffice and provided that such reproduction and distribution is performed for non-commercial purposes.

Tamer Sahin
<http://www.securityoffice.net>

-----BEGIN PGP SIGNATURE-----

Version: 2.6

iQEVAwUAPfThqPpL5ibJRTtBAQHVAgf6AnmCPT8iqOTMcYjU3RynwG7dhe8SkKQV
dWjVgc/rY3X1NReDom3DkgyaxUKp8mPY11O5Gy1z2JfWhjMVmIAMsop4op2O+eLw
M5bb8MTP5K6jiNzc9EY0YBgA0LHaisJ4zf3PaCWzyaj8r+JUW3Ww16f3JNQZyE8A
1uKHenmeuyAW3tQQC4uYxkv2JDHPizTrGmxh3xxSk+INytjAfauvCGhZ83Yj1dz
sdE/brtBc+LnUsrPSHvLcFnBEuTHjx7aE8GUnKmBhZAZKek3AzIcIshCjo/WgNLI
yu8eEmooF7X55zB/0wy26qPYy79aRSho+oqsoWOFkVkcjn3adKF+RQ==
=oPND

-----END PGP SIGNATURE-----