



Contact:
Kevin Gallagher
Gallagher Group Communications
925-831-1041
kevin@gg-comm.com

MU DYNAMICS DISCOVERS REMOTE DENIAL OF SERVICE VULNERABILITY IN WIDELY USED VOICE OVER IP ReSIProcate PRODUCT

SUNNYVALE, CA – July 11, 2008 – Mu Dynamics, a pioneer in helping network operators and their vendors eliminate downtime through proactive service assurance, has discovered and helped remediate a new programming flaw in ReSIProcate: A remotely exploitable Denial of Service vulnerability. The ReSIProcate components, particularly the [SIP stack](#), is currently used in several [Voice over IP \(VoIP\)](#) commercial and open-source products. The project exists to maintain a complete, correct, and commercially usable implementation of SIP and a few related protocols.

<http://labs.mudynamics.com/advisories.html>

Affected Products/Versions: repro SIP proxy/registrar 1.3.2; however any product using the ReSIProcate SIP stack 1.3.2 may also be vulnerable.

http://www.resiprocate.org/ReSIProcate_1.3.2_Release

Product Overview: ReSIProcate is a SIP stack. SIP is a protocol used for session establishment that is widely used to support voice-over-IP telephony. “repro” is a SIP proxy/registrar that uses the ReSIProcate SIP stack. <http://www.resiprocate.org/>

Vulnerability Details: A malformed INVITE or OPTIONS message to the “repro” SIP proxy/ registrar can crash the process. The crash is caused by an assertion failure that occurs when the domain name in the request line URI is too long.

Vendor Response /Solution: Update to 1.3.3, available from <https://www.resiprocate.org/files/pub/reSIProcate/releases/>

This bug was also fixed by the ReSIProcate development team in SVN on April 23, 2008 (revision 7628).

History:
July 1, 2008 - First contact with vendor
July 1, 2008 - Vendor acknowledges vulnerability

July 3, 2008 - Vendor releases 1.3.3
July 10, 2008 - Advisory released
Mu-4000 vector: *.request-line.line.dsv.uri.body.string.append-overflow

Credit: This vulnerability was discovered by the Mu Dynamics research team.
<http://labs.mudynamics.com/pgpkey.txt>

Related Content:

[Mu VoIP Case Study](http://www.mudynamics.com/assets/docs/voip_case_study.pdf) - http://www.mudynamics.com/assets/docs/voip_case_study.pdf

[Mu SIP Page](http://www.mudynamics.com/solutions/next-gen-ip-services/sip.html) - <http://www.mudynamics.com/solutions/next-gen-ip-services/sip.html>

[Mu DoS Module](http://www.mudynamics.com/products/modules/dos.html) - <http://www.mudynamics.com/products/modules/dos.html>

[Mu DoS Demonstration](http://www.mudynamics.com/products/demo.html) - <http://www.mudynamics.com/products/demo.html>

About Mu Dynamics

Mu Dynamics proactively eliminates the high cost of service, application and network downtime. Mu's solution automates a systematic and repeatable process that identifies hard-to-detect sources of potential downtime within IP services, applications, and underlying networks. The award-winning Mu solution is deployed at more than 100 locations, primarily at leading global service providers, cable operators and network product vendors. Headquartered in Sunnyvale, California, Mu is backed by leading venture capital firms that include Accel Partners, Benchmark Capital, DAG Ventures and Focus Ventures. <http://www.mudynamics.com>

###