

[Full-disclosure] [MU-200704-01] Pre-Authentication Vulnerability in Mac OS X RPC runtime library

Source: <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2007-04/msg00594.html>

- *From:* noreply@xxxxxxxxxxxxxxxx
 - *Date:* Fri, 20 Apr 2007 22:57:09 +0100 (BST)
-

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

Hash: SHA1

Pre-Authentication Vulnerability in Mac OS X RPC runtime library [MU-200704-01]
April 20, 2007

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

Affected Product/Versions:

Mac OS X v10.3.9,
Mac OS X Server v10.3.9,
Mac OS X v10.4.9,
Mac OS X Server v10.4.9

Product Overview:

"Portmap is a server that converts RPC program numbers into DARPA protocol port numbers. It must be running in order to make RPC calls.

When an RPC server is started, it will register with the portmap the port number it is listening to, and what RPC program numbers it is prepared to serve. When a client wishes to make an RPC call to a given program number, it will first contact portmap on the server machine to determine the port number where RPC packets should be sent."

Vulnerability Details:

An integer overflow vulnerability exists in the RPC runtime library (libinfo) that handles AUTH_UNIX authentication. By sending maliciously-crafted requests to the any RPC service (portmap, mount, nfs, etc), a remote attacker can trigger the overflow which may lead to arbitrary code execution as the 'daemon' user.

The problem is a signed integer issue in parsing XDR strings. In general an XDR string contains a 4-byte big-endian length followed by the string. Any

[Full-disclosure] [MU-200704-01] Pre-Authentication Vulnerability in Mac OS X RPC runtime library

length greater than 0x80000000 results in a negative length which is then passed into a memcpy whose length can be controlled by the attacker.

The vulnerability can be triggered by sending the malicious AUTH_UNIX packets to the NULL procedure of any enabled RPC service.

Vendor Response / Solution:

All users of RPC on OS X are recommended to immediately apply the security updates available from the following URL:

<http://docs.info.apple.com/article.html?artnum=61798>

Mu Security would like to thank Apple for remediation of these vulnerabilities.

History:

12/18/06 – First contact with the vendor
04/09/07 – Fix available for the vulnerabilities
04/20/07 – Advisory released

Credit:

This vulnerability was discovered by the Mu Security research team.

<http://labs.musecurity.com/pgpkey.txt>

Mu Security offers a new class of security analysis system, delivering a rigorous and streamlined methodology for verifying the robustness and security readiness of any IP-based product or application. Founded by the pioneers of intrusion detection and prevention technology, Mu Security is backed by preeminent venture capital firms that include Accel Partners, Benchmark Capital and DAG Ventures. The company is headquartered in Sunnyvale, CA. For more information, visit the company's website at <http://www.musecurity.com>.

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

Version: GnuPG v1.4.6 (Darwin)

iD8DBQFGKP8E+aa9jJz2VeARAIFcAJ92sTKVKx6QVf9Mq7YTta/1iBggA+QCfVxwq
wBLtHG5ksNFJ7Nm8QpyYuQI=
=GMPf

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

Full-Disclosure – We believe in it.

Charter: <http://lists.grok.org.uk/full-disclosure-charter.html>

Hosted and sponsored by Secunia – <http://secunia.com/>

[Full-disclosure] [MU-200704-01] Pre-Authentication Vulnerability in Mac OS X RPC runtime library