===

CERT(sm) Advisory CA-96.13
July 4, 1996

Topic: ID4 virus, Alien/OS Vulnerability

- -

The CERT Coordination Center has received reports of weaknesses in Alien/OS that can allow species with primitive information sciences technology to initiate denial-of-service attacks against MotherShip(tm) hosts. One report of exploitation of this bug has been received.

When attempting takeover of planets inhabited by such races, a trojan horse attack is possible that permits local access to the MotherShip host, enabling the implantation of executable code with full root access to mission-critical security features of the operating system.

The vulnerability exists in versions of EvilAliens' Alien/OS 34762.12.1 or later, and all versions of Microsoft's Windows/95. CERT advises against initiating further planet takeover actions until patches are available from these vendors. If planet takeover is absolutely necessary, CERT advises that affected sites apply the workarounds as specified below.

As we receive additional information relating to this advisory, we will place it in

        ftp://info.cert.org/pub/cert_advisories/CA-96.13.README

We encourage you to check our README files regularly for updates on advisories that relate to your site.

- -

I.   Description

Alien/OS contains a security vulnerability, which strangely enough can be exploited by a primitive race running Windows/95. Although Alien/OS has been extensively field tested over millions of years by EvilAliens, Inc., the bug was only recently discovered during a routine invasion of a backwater planet. EvilAliens notes that the operating system had never before been tested against a race with "such a kick-ass president."

The vulnerability allows the insertion of executable code with root access to key security features of the operating system. In particular, such code can disable the NiftyGreenShield (tm) subsystem, allowing child processes to be terminated by unauthorized users.

Additionally, Alien/OS networking protocols can provide a low-bandwidth covert timing channel to a determined attacker.

II.   Impact

Non-privileged primitive users can cause the total destruction of your entire invasion fleet and gain unauthorized access to files.

III. Solution

EvilAliens has supplied a workaround and a patch, as follows:

A. Workaround

To prevent unauthorized insertion of executables, install a firewall to selectively vaporize incoming packets that do not contain valid aliens. Also, disable the "Java" option in Netscape.

To eliminate the covert timing channel, remove untrusted hosts from routing tables. As tempting as it is, do not use target species' own satellites against them.

B. Patch

As root, install the "evil" package from the distribution tape.

(Optionally) save a copy of the existing /usr/bin/sendmail and modify its permission to prevent misuse.

- -

The CERT Coordination Center thanks Jeff Goldblum and Fjkxdtssss for providing information for this advisory.

- -

If you believe that your system has been compromised, contact the CERT Coordination Center or your representative in the Forum of Incident Response and Security Teams (FIRST).

We strongly urge you to encrypt any sensitive information you send by email.
The CERT Coordination Center can support a shared DES key and PGP. Contact the CERT staff for more information.

Location of CERT PGP key
ftp://info.cert.org/pub/CERT_PGP.key

CERT Contact Information
- - ------------------------

Email   cert@cert.org

Phone   +1 412-268-7090 (24-hour hotline)
CERT personnel answer 8:30-5:00 p.m. EST
(GMT-5)/EDT(GMT-4), and are on call for
emergencies during other hours.

Fax   +1 412-268-6989

Postal address
CERT Coordination Center
Software Engineering Institute
Carnegie Mellon University
Pittsburgh PA 15213-3890
USA

CERT publications, information about FIRST representatives, and other security-related information are available for anonymous FTP from
http://www.cert.org/
ftp://info.cert.org/pub/

CERT advisories and bulletins are also posted on the USENET newsgroup
comp.security.announce

To be added to our mailing list for CERT advisories and bulletins, send your email address to
cert-advisory-request@cert.org

[Parent]

HTML by Area 51 Researech Center, 7/17/96.