

[VulnWatch] Etherleak: Ethernet frame padding information leakage (A010603-1)

Source: <http://www.derkeiler.com/Mailing-Lists/VulnWatch/2003-01/0010.html>

From: @stake Advisories (@stake)

Date: 01/06/03

Date: Mon, 06 Jan 2003 12:24:19 -0500

From: "@stake Advisories" <advisories@atstake.com>

To: vulnwatch@vulnwatch.org

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

Hash: SHA1

@stake, Inc.
www.atstake.com

Security Advisory

Advisory Name: Etherleak: Ethernet frame padding information leakage

Release Date: 01/06/2003

Application: Ethernet device driver software

Platform: Multiple

Severity: Information disclosure

Authors: Ofir Arkin <ofir@sys-security.com>

Josh Anderson

Vendor Status: Multiple vendors alerted via CERT Coordination Center

CVE Candidate: CAN-2003-0001

Reference: www.atstake.com/research/advisories/2003/a010603-1.txt

Overview:

Multiple platform ethernet Network Interface Card (NIC) device drivers incorrectly handle frame padding, allowing an attacker to view slices of previously transmitted packets or portions of kernel memory. This vulnerability is the result of incorrect implementations of RFC requirements and poor programming practices, the combination of which results in several variations of this information leakage vulnerability.

The simplest attack using this vulnerability would be to send ICMP echo messages to a machine with a vulnerable ethernet driver.

Portions of kernel memory will be returned to the attacker in the padding of the reply messages. During testing we have found that the portions returned are typically snippets of network traffic

VulnWatch: [VulnWatch] Etherleak: Ethernet frame padding information leakage (A010603-1)

that the vulnerable machine is handling. This attack can allow an attacker to see portions of the traffic that a router or firewall is handling on network segments the attacker has no direct access too. It is important to note that the attacker must be on the same ethernet network as the vulnerable machine to receive the ethernet frames.

Details:

@stake has prepared a detailed report on this issue. The vulnerability is explored in its various manifestations through code examples and packet captures.

Report available at:

www.atstake.com/research/advisories/2003/atstake_etherleak_report.pdf

Vendor Response:

Multiple platform and hardware vendors were contacted via the CERT Coordination Center on 06/25/02. Detailed vendor response information is available in CERT vulnerability note VU#412115.

Recommendation:

Contact the vendor of your ethernet device drivers or your hardware vendor for a patch.

End to end encryption technologies such as SSL, IPSEC, and SSH should be used when transmitting sensitive data over a network. Using encryption will help protect against this issue partly. It is not a complete solution because the kernel data leaked in the ethernet frame padding is not always the IP packet data portion of a previous frame. Sometimes it is unencrypted IP header information or other kernel memory.

Common Vulnerabilities and Exposures (CVE) Information:

The Common Vulnerabilities and Exposures (CVE) project has assigned the following names to these issues. These are candidates for inclusion in the CVE list (<http://cve.mitre.org>), which standardizes names for security problems.

CAN-2003-0001 Ethernet frame padding information leakage

@stake Vulnerability Reporting Policy:
<http://www.atstake.com/research/policy/>

@stake Advisory Archive: <http://www.atstake.com/research/advisories/>

VulnWatch: [VulnWatch] Etherleak: Ethernet frame padding information leakage (A010603-1)

PGP Key:

http://www.atstake.com/research/pgp_key.asc

Copyright 2003 @stake, Inc. All rights reserved.

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

Version: PGP 8.0

iQA/AwUBPhmc+Ee9kNIfAm4yEQKyjACgnvi0ZuRUb94nfcG0zMHPzl6XdZQAn1tG

TXcUNSc0uLgCvhUp0vQAU7+J

=3Dtx

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