

[REVS] Access over Ethernet: Insecurities in AoE

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2006-09/msg00034.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxx>
 - *Date:* 28 Sep 2006 09:01:37 +0200
-

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.

<http://www.securiteam.com/maillinglist.html>

Access over Ethernet: Insecurities in AoE

SUMMARY

ATA over Ethernet (AoE) is an open standards based protocol which allows direct network access to disk drives by client hosts. AoE has been incorporated into the mainstream Linux kernel, recently been the subject of a Slashdot article, and it appears that it is a SAN technology which is here to stay. This paper investigates the insecurities present in the AoE protocol and suggests how you can deploy AoE infrastructure without worrying about a wide scale compromise.

DETAILS

What is AoE?

ATA over Ethernet (AoE) is an open standards based protocol that allows direct network access to disk drives by client hosts. It has been developed by Coraid (The Linux Storage People) as a SAN technology and it has been adopted for use by many Universities and US Government agencies. Coraid provides a hardware AoE cluster implementation called EtherDrive . The Coraid website has downloadable case studies from NASA and the University of Alaska. The claim is that AoE delivers a simple, high performance, low cost alternative to iSCSI and FibreChannel for networked block storage by eliminating the processing overhead of TCP/IP.

[REVS] Access over Ethernet: Insecurities in AoE

Support for AoE is native in the linux kernel as of version 2.6.11.

AoE is a stateless protocol which consists of request messages sent to the AoE server and reply messages returned to the client host. Some messages contain ATA commands, and any data associated with the transaction. Other messages relate to the Config/Query feature of the protocol, to set and query a small amount of out of band data. The formats of these messages are simple and have two forms: ATA messages, and Config/Query messages. Both share a common header format that facilitates network delivery. AoE utilizes the standard Ethernet MAC header for IEEE 802.3 Ethernet frames. AoE has a registered Ethernet type of 0x88A2.

ADDITIONAL INFORMATION

The information has been provided by

<