

[NT] Sygate Enforcer Unauthenticated Broadcast Bypassing

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-08/0034.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 08/11/04

To: list@securiteam.com

Date: 11 Aug 2004 17:35:04 +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>

Sygate Enforcer Unauthenticated Broadcast Bypassing

SUMMARY

<http://www.sygate.com/products/universal_enforcement.htm> Sygate Enforcers are described as "network gateway devices that enforce host integrity at network access points". Architecturally they function as an authenticated, packet-filtering firewall device. The Enforcer interacts with the Sygate Security Agent (SAA [the personal firewall component]) product and limits access to protected networks/hosts to authenticated clients that comply with a predefined policy.

In practice, the Enforcer does not limit broadcast traffic (both local-net and all-nets) from passing through prior to authentication, allowing hosts that are protected by the Enforcer to still be attacked.

DETAILS

Vulnerable Systems:

* Sygate Enforcer version prior to 3.5MR1

CVE Information:

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0593>>

Securiteam: [NT] Sygate Enforcer Unauthenticated Broadcast Bypassing

CAN-2004-0593

ADDITIONAL INFORMATION

The information has been provided by <mailto:martin.oneal@corsaire.com>
Martin O'Neal.

The original article can be found at:

<<http://www.corsaire.com/advisories/c031120-003.txt>>

<http://www.corsaire.com/advisories/c031120-003.txt>

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

list-unsubscribe@securiteam.com

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====

=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.