

[REVS] Common Firewall Configuration Errors

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-10/0056.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 10/17/04

To: list@securiteam.com

Date: 17 Oct 2004 16:13:09 +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>

Common Firewall Configuration Errors

SUMMARY

The protection that firewalls provide is only as good as the policy they are configured to implement. Analysis of real configuration data shows that corporate firewalls are often enforcing rule sets that violate well established security guidelines.

DETAILS

Excerpt:

Firewalls are the cornerstone of corporate intranet security. Once a company acquires a firewall, a system administrator must configure and manage it according to a security policy that meets the company's needs. Configuration is a crucial task, probably the most important factor in the security firewall provides.

In this article, Avishai Wool focus on rule sets for

<<http://www.checkpoint.com>> Check Point's FireWall-1 product and, specifically, on 12 possible misconfigurations that would allow access beyond a typical corporation's network security policy. By documenting the frequency of misconfigurations in actual firewall data, Avishai Wool was able to check whether the configuration quality is correlated with other factors specifically, the operating on which the firewall runs, the firewall's software version, and a new measure of rule-set complexity.

Securiteam: [REVS] Common Firewall Configuration Errors

See the full article at:

<<http://www.eng.tau.ac.il/~yash/computer2004.pdf>> A Quantitative Study of Firewall Configuration Errors

ADDITIONAL INFORMATION

The original article can be found at:

<<http://www.eng.tau.ac.il/~yash/computer2004.pdf>> A Quantitative Study of Firewall Configuration Errors

=====

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.