

[NT] Insecure Default File System Permissions n Microsoft Versions of Kerio Software

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-12/0044.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 12/16/04

To: list@securiteam.com

Date: 16 Dec 2004 14:11:46 +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>

Insecure Default File System Permissions n Microsoft Versions of Kerio Software

SUMMARY

As a result of its collaboration relationship the Secure Computer Group (SCG) along with dotpi.com Research Labs have determined the following security issue on some Kerio Software.

Kerio WinRoute Firewall, Kerio ServerFirewall and Kerio MailServer are installed by default under 'Program Files' system folder. No change is done to the ACLs after the installation process. As a result, anyone belonging to the 'Power Users' system group would be able to modify binary files of services running as LOCALSYSTEM, drop malicious DLLs the plug-ins folder or perform any change on the XML files where the service settings are stored.

System administrators should enforce ACL security settings in order solve this problem. It is also highly recommended to verify this settings as part of the planning, installation, hardening and auditing processes.

New versions of the software solve this an other minor problems so it is upgrade its highly recommended.

Securiteam: [NT] Insecure Default File System Permissions n Microsoft Versions of Kerio Software

DETAILS

Vulnerable Systems:

- * Kerio WinRoute Firewall version 6.0.8 and prior
- * Kerio ServerFirewall version 1.0.0 and prior
- * Kerio MailServer version 6.0.4 and prior

Immune Systems:

- * Kerio WinRoute Firewall version 6.0.9
- * Kerio ServerFirewall version 1.0.1
- * Kerio MailServer version 6.0.5

CVE Information:

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-1023>>
 CAN-2004-1023

Solutions and recommendations:

Enforce the file system ACLs and/or upgrade to the latest versions:

- * Kerio WinRoute Firewall 6.0.9
- * Kerio ServerFirewall 1.0.1
- * Kerio MailServer 6.0.5

As in any other case, follow, as much as possible, the Industry 'Best Practices' on Planning, Deployment and Operation on this kind of services.

ADDITIONAL INFORMATION

The information has been provided by <mailto:scg@udc.es> Secure Computer Group.

The original article can be found at:

<<http://research.tic.udc.es/scg/advisories/20041214-2.txt>>
<http://research.tic.udc.es/scg/advisories/20041214-2.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.