

Securiteam: [NT] Multiple Vulnerabilities in Kerio Product (Information Disclosure, DoS)

[NT] Multiple Vulnerabilities in Kerio Product (Information Disclosure, DoS)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-05/0001.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 05/01/05

To: list@securiteam.com

Date: 1 May 2005 17:53:15 +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>

Multiple Vulnerabilities in Kerio Product (Information Disclosure, DoS)

SUMMARY

<<http://www.kerio.com/>> Kerio WinRoute Firewall, Kerio Personal Firewall and Kerio MailServer drive a local/remote administration protocol in order to manage the service.

By using a brute force attack technique on Kerio WinRoute Firewall, Kerio Personal Firewall and Kerio MailServerit administration protocol it is possible to retrieve the administrative password from a remote installation. Further, the Kerio products are also vulnerable in to a denial of service in their pre-authentication state.

DETAILS

Vulnerable Systems:

- * Kerio WinRoute Firewall version 6.0.10 and prior
- * Kerio Personal Firewall version 4.1.2 and prior
- * Kerio MailServer version 6.0.8 and prior

Immune Systems:

- * Kerio WinRoute Firewall version 6.0.11 and above

Securiteam: [NT] Multiple Vulnerabilities in Kerio Product (Information Disclosure, DoS)

- * Kerio Personal Firewall version 4.1.3 and above
- * Kerio MailServer version 6.0.9 and above

Information Disclosure:

The Kerio products allow local/remote administration of the products via an special administration protocol.

This protocol can be abused in through a brute forcing technique to retrieve the administrator password. Passwords that are 1–5 characters long could be obtained quickly. Longer passwords make the attack not practically feasible.

The logging component of the software can loose up to 40% of the events when the attack is in place.

An abuse is possible if attacker have access to the administration ports:

- * TCP/UDP 44333 – Kerio WinRoute Firewall Administration
- * TCP/UDP 44334 – Kerio Personal Firewall Administration
- * TCP/UDP 44337 – Kerio MailServer Administration

Special attention should be taken on environments on which NT, Active Directory or Open Directory integration is in place. GINA.DLL re–login delay features are bypassed and therefore the brute forcing procedure is considerably quicker.

Workaround:

In order solve this problem, system administrators should enforce network ACL security settings and user password policies. It is also highly recommended to verify this settings as part of the planning, installation, hardening and auditing processes.

Denial of Service:

The same protocol as described above can be abused in its pre–authentication state to compute unexpected conditions and perform cryptographic operations, resulting in system resources get exhausted and the system becoming unresponsive.

NOTE: The limit of maximum number of user connections can also be used to perform a service denial of service and that no valid authentication is required for this to succeed.

The logging component of the software ignores any event related with this attack.

In order to preform an attack, attacker need access to the administration ports:

- * TCP/UDP 44333 – Kerio WinRoute Firewall Administration
- * TCP/UDP 44334 – Kerio Personal Firewall Administration
- * TCP/UDP 44337 – Kerio MailServer Administration

Securiteam: [NT] Multiple Vulnerabilities in Kerio Product (Information Disclosure, DoS)

Workaround:

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

CVE Information:

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-1062>>
CAN-2005-1062
<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-1063>>
CAN-2005-1063

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/20050429-1.txt>>
<http://research.tic.udc.es/scg/advisories/20050429-1.txt> and
<<http://research.tic.udc.es/scg/advisories/20050429-2.txt> >
<http://research.tic.udc.es/scg/advisories/20050429-2.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.