CERT Advisory CA-2001-17 Check Point RDP Bypass Vulnerability

Original release date: July 09, 2001
Last revised: July 12, 2001
Source: CERT/CC

A complete revision history is at the end of this file.

Systems Affected

- Check Point VPN-1 and FireWall-1 Version 4.0 & 4.1

Overview

A vulnerability in Check Point FireWall-1 and VPN-1 may allow an intruder to pass traffic through the firewall on port 259/UDP.

I. Description

Inside Security GmbH has discovered a vulnerability in Check Point FireWall-1 and VPN-1 that allows an intruder to bypass the firewall. The default FireWall-1 management rules allow arbitrary RDP connections to traverse the firewall.

FireWall-1 and VPN-1 include support for RDP, but they do not provide adequate security controls. Quoting from the advisory provided by Inside Security GmbH:

> *By adding a faked RDP header to normal UDP traffic any content can be passed to port 259 on any remote host on either side of the firewall.*

For more information, see the Inside Security GmbH security advisory, available at

http://www.inside-security.de/advisories/fw1_rdp.html

Although the CERT/CC has not seen any incident activity related to this vulnerability, we do recommend that all affected sites upgrade their Check Point software as soon as possible.

II. Impact

An intruder can pass UDP traffic with arbitrary content through the firewall on port 259 in violation of implied security policies.

If an intruder can gain control of a host inside the firewall, he may be able to use this vulnerability to tunnel arbitrary traffic across the firewall boundary.

Additionally, even if an intruder does not have control of a host inside the firewall, he may be able to use this vulnerability as a means of exploiting another vulnerability in software listening passively on the internal network.

Finally, an intruder may be able to use this vulnerability to launch certain kinds of denial-of-service attacks.

III. Solutions

Install a patch from Check Point Software Technologies. More information is available in Appendix A.

Until a patch can be applied, you may be able to reduce your exposure to this vulnerability by configuring your router to block access to 259/UDP at your network perimeter.

Appendix A

Check Point

Check Point has issued an alert for this vulnerability at

http://www.checkpoint.com/techsupport/alerts/rdp.html

Download the patch from Check Point's web site:

http://www.checkpoint.com/techsupport/downloads.html

Appendix B. - References

1. http://www.inside-security.de/advisories/fw1_rdp.html
2. http://www.kb.cert.org/vuls/id/310295

Our thanks to Inside Security GmbH for the information contained in their advisory.

This document was written by Ian A. Finlay. If you have feedback concerning this document, please send email to:

mailto:cert@cert.org?Subject=Feedback CA-2001-17 [VU#310295]

Revision History

```
July 09, 2001: Initial Release
July 09, 2001: Removed references to RFC's describing RDP. Specifically,
               we removed the references to RFC-908 and RFC-1151.

July 09, 2001: Added reference to Check Point's security document.
July 12, 2001: Added version 4.0 to systems affected section.
```