US-CERT

UNITED STATES COMPUTER EMERGENCY READINESS TEAM

US-CERT Advisory- 08-05: Vulnerability in the PDF distiller of the BlackBerry Attachment Service for the BlackBerry Enterprise Server

Published: July 18, 2008

OVERVIEW

Research In Motion (RIM) has released a Security Advisory to address a vulnerability in the BlackBerry Enterprise Server. This vulnerability is due to the improper processing of PDF files within the distiller component of the BlackBerry Attachment Service. By convincing a user to open a maliciously crafted PDF attachment on a BlackBerry smartphone, an attacker may be able to execute arbitrary code on the system running the BlackBerry Attachment Service.

Resources

BlackBerry Security Advisory
KB15766

US-CERT Current Activity
http://www.us-cert.gov/current/index.html#blackberry_security_advisory

Cyber Security Tip ST04-010, "Using Caution with Email Attachments."

DETAILS

According to the advisory, a security vulnerability exists in the PDF distiller of some released versions of the BlackBerry Attachment Service. This vulnerability could enable a malicious individual to send an email message containing a specially crafted PDF file, which when opened for viewing on a BlackBerry smartphone, could cause memory corruption and possibly lead to arbitrary code execution on the computer that the BlackBerry Attachment Service runs on.

SOLUTION

US-CERT recommends that organizations consider upgrading to BlackBerry Enterprise Server software version 4.1 Service Pack 6 (4.1.6).

RIM has also issued an interim security software update that resolves this vulnerability. Visit http://www.blackberry.com/go/serverdownloads to obtain the interim security software update for affected release versions earlier than BlackBerry Enterprise Server software version 4.1.6.

If the updates cannot be applied, US-CERT recommends that organizations follow the workarounds listed in the BlackBerry advisory. This includes disabling PDF files from being processed in a BlackBerry Enterprise Environment. To view the complete list of instructions on how to change the settings of the BlackBerry Attachment Service, please review the security advisory.

Organizations should follow their established internal procedures if any suspected malicious activity is observed, and report their findings to US-CERT for correlation against other incidents. US-CERT also reminds organizations that proper impact analysis should be performed prior to taking defensive measures.

Organizations should also remind users of the following best practices:

- Do not trust or open unsolicited email
- Treat all email attachments with caution
- Do not click links in unsolicited email messages
- Install and maintain up to date anti-virus software
- Always ensure that your system is fully patched

Stay informed and involved by subscribing to the products included in the US-CERT National Cyber Alert System. To learn more, visit http://www.us-cert.gov/cas/signup.html.

For any questions or to report an incident related to this advisory, please contact US-CERT at:

Email: soc@us-cert.gov
Voice: 1-888-282-0870
Incident Reporting Form: https://forms.us-cert.gov/report/