Adobe Acrobat And Reader CVE-2013-0640 Remote Code Execution Vulnerability

Risk
High

Date Discovered
February 12, 2013

Description
Adobe Acrobat and Reader are prone to an unspecified remote code-execution vulnerability. An attacker can exploit this issue to execute arbitrary code within the context of the affected application or to crash the application. Limited information is known about this issue. We will update this BID as soon as more information becomes available. Adobe Acrobat and Reader versions 11.0.1 and prior are vulnerable.

Technologies Affected
- Adobe Acrobat (for Macintosh) 10.1.5
- Adobe Acrobat (for Macintosh) 11.0.1
- Adobe Acrobat (for Macintosh) 9.5.3
- Adobe Acrobat (for Windows) 10.1.5
- Adobe Acrobat (for Windows) 11.0.1
- Adobe Acrobat (for Windows) 9.5.3
- Adobe Acrobat 10.0
- Adobe Acrobat 10.0.1
- Adobe Acrobat 10.0.2
- Adobe Acrobat 10.0.3
- Adobe Acrobat 10.1
- Adobe Acrobat 10.1.1
- Adobe Acrobat 10.1.2
- Adobe Acrobat 10.1.3
- Adobe Acrobat 10.1.4
- Adobe Acrobat 11.0.0
- Adobe Acrobat 9.5

- Adobe Acrobat 9.5.1
- Adobe Acrobat 9.5.2
- Adobe Acrobat Reader (for Macintosh) 9.5.3
- Adobe Reader (for Macintosh) 10.0.1
- Adobe Reader (for Macintosh) 10.1.5
- Adobe Reader (for Windows) 10.0.1
- Adobe Reader (for Windows) 10.1.5
- Adobe Reader (for Windows) 9.5.3
- Adobe Reader 10.0
- Adobe Reader 10.0.1
- Adobe Reader 10.0.2
- Adobe Reader 10.0.3
- Adobe Reader 10.1
- Adobe Reader 10.1.1
- Adobe Reader 10.1.2
- Adobe Reader 10.1.3
- Adobe Reader 10.1.4
- Adobe Reader 11.0
- Adobe Reader 11.0.1
- Adobe Reader 9.5
- Adobe Reader 9.5.1
- Adobe Reader 9.5.2
- Gentoo Linux
- Red Hat Enterprise Linux Desktop Supplementary 5 Client
- Red Hat Enterprise Linux Desktop Supplementary 6
- Red Hat Enterprise Linux Server Supplementary 6
- Red Hat Enterprise Linux Supplementary 5 Server
- Red Hat Enterprise Linux Workstation Supplementary 6
- SuSE SUSE Linux Enterprise Desktop 10 SP4
- SuSE SUSE Linux Enterprise Desktop 11 SP2
- SuSE openSUSE 11.4
- SuSE openSUSE 12.1

Recommendations

Run all software as a nonprivileged user with minimal access rights.
To reduce the impact of latent vulnerabilities, run all applications with the minimal amount of privileges required for functionality.

Deploy network intrusion detection systems to monitor network traffic for malicious activity.
Deploy NIDS to monitor network traffic for signs of anomalous or suspicious activity. This includes but is not limited unexplained incoming and outgoing traffic. This may indicate exploit attempts or activity that results from successful exploits.

Do not accept or execute files from untrusted or unknown sources.
To limit exposure to these and other latent vulnerabilities, never handle files that originate from unfamiliar or untrusted sources.

Do not follow links provided by unknown or untrusted sources.
To reduce the likelihood of successful exploits, never visit sites of questionable integrity or follow links provided by unfamiliar or untrusted sources.

Updates are available. Please see the references or vendor advisory for more information.

References

- Adobe - Adobe Homepage
- Adobe - Adobe Reader and Acrobat Vulnerability Report
- Adobe - Adobe Reader Homepage
- FireEye - IN TURN, IT'S PDF TIME

Credits

FireEye