National Computer Board

Computer Emergency Response Team of Mauritius (CERT-MU)

Targeted Security Alert

Multiple Vulnerabilities in Adobe Products

Original Issue Date: May 13, 2015

Severity Rating: High

Systems Affected:

- Adobe Flash Player 17.0.0.169 and earlier versions
- Adobe Flash Player 13.0.0.281 and earlier 13.x versions
- Adobe Flash Player 11.2.202.457 and earlier 11.x versions
- AIR Desktop Runtime 17.0.0.144 and earlier versions
- AIR SDK and SDK & Compiler 17.0.0.144 and earlier versions

Description:

Multiple vulnerabilities have been identified in Adobe products and can be exploited by remote attackers to cause execution of code and bypass restrictions on Javascript API execution. The vulnerabilities reported are as follows:

- Memory corruption vulnerabilities exist and the vulnerabilities could be exploited by remote attackers to cause execution of arbitrary code.
- A heap overflow vulnerability occur which could lead to code execution.
- A time-of-check time-of-use (TOCTOU) race condition exists and this could be exploited by remote attackers to bypass Protected Mode in Internet Explorer.
- Resolve validation bypass issues exist that could be exploited by remote attackers to write arbitrary data to the file system under user permissions.
- An integer overflow vulnerability occurs and this could be exploited by remote attackers to cause execution of arbitrary code.
- A type confusion vulnerability exists which could be exploited to cause code execution.
- A use-after-free vulnerability occurs that could be exploited by remote attackers to cause code execution.

- Memory leak vulnerabilities exist that could be exploited to bypass ASLR.
- A security bypass vulnerability exist that could be exploited by remote attackers to cause information disclosure and provide additional hardening.

Workarounds:

Users are advised to apply the following updates:

- Adobe Flash Player desktop runtime for Windows and Macintosh should update to Adobe Flash Player 17.0.0.188
- Adobe Flash Player Extended Support Release should update to Adobe Flash Player 13.0.0.289
- Adobe Flash Player for Linux should update to Adobe Flash Player 11.2.202.460
- Adobe Flash Player installed with Google Chrome, as well as Internet Explorer on Windows 8.x, will automatically update to version 17.0.0.188
- Adobe AIR desktop runtime should update to version 17.0.0.172
- Adobe AIR SDK and AIR SDK & Compiler should update to version 17.0.0.172

More information about the updates is available on:
https://helpx.adobe.com/security/products/flash-player/apsb15-09.html

Vendor Information
Adobe
www.adobe.com

References

Adobe Security Bulletin
https://helpx.adobe.com/security/products/flash-player/apsb15-09.html

SC Magazine
http://www.scmagazine.com/adobe-plugs-critical-bugs-in-reader-acrobat-and-flash-player/article/414279/

Please note that the members who do not want to receive the security alert, they can unsubscribe from CERT-MU mailing list by sending an e-mail to the following address: unsubscribe@cert.ncb.mu

For more information please contact CERT-MU team on:

Hotline No: (+230) 800 2378

Fax No: (+230) 208 0119

Gen. Info: contact@cert.ncb.mu

Incident: incident@cert.ncb.mu

Website: www.cert-mu.org.mu