SA62621
Adobe Flash Player /AIR Multiple Vulnerabilities

Secunia
Stay Secure

Secunia ID:	SA62621
Title:	Adobe Flash Player / AIR Multiple Vulnerabilities
Release date:	2015-03-13
Last update	2015-05-07

Criticality:	Highly critical
Impact:	Security bypass System access
Where:	From remote
Solution status:	Vendor patched
Software:	Adobe AIR 17.x Adobe Flash Player 11.x Adobe Flash Player 13.x
Secunia CVSS Score:	10 (AV:N/AC:L/Au:N/C:C/I:C/A:C/E:U/RL:OF/RC:C)
CVE Reference(s):	CVE-2015-0332 CVE-2015-0333 CVE-2015-0334 CVE-2015-0335 CVE-2015-0336 CVE-2015-0337 CVE-2015-0338 CVE-2015-0339 CVE-2015-0340 CVE-2015-0341 CVE-2015-0342

Description:

Multiple vulnerabilities have been reported in Adobe Flash Player and Adobe AIR, which can be exploited by malicious people to bypass certain security restrictions and compromise a user's system.

1. An unspecified error can be exploited to corrupt memory.
2. Another unspecified error can be exploited to corrupt memory.
3. Another unspecified error can be exploited to corrupt memory.
4. Another unspecified error can be exploited to corrupt memory.
5. A type confusion error related to the constructors of the XML and XMLNode classes can be exploited to corrupt memory.
6. A type confusion error in the ActionScript 2 NetConnection class can be exploited to corrupt memory.
7. An unspecified error can be exploited to bypass the cross-domain policy.
8. An unspecified error can be exploited to bypass the file upload restriction.
9. An integer overflow error can be exploited to corrupt memory.
10. A use-after-free error when handling AVSS objects can be exploited to corrupt memory.
11. A use-after-free error can be exploited to corrupt memory.

Successful exploitation of the vulnerabilities #1 through #6 and #9 through #11 may allow execution of arbitrary code.

The vulnerabilities are reported in the following products and versions:

* Adobe Flash Player Extended Support Release versions 13.x through 13.0.0.269.
* Adobe Flash Player for Linux versions 11.2.202.442 and prior.
* Adobe IR Desktop runtime, AIR SDK, AIR SDK & Compiler, and AIR Android versions 17.0.0.124 and prior.

SA62621
Adobe Flash Player /AIR Multiple Vulnerabilities

Secunia
Stay Secure

Description:

Update to a fixed version.

Adobe Flash Player Extended Support Release:

Update to version 13.0.0.277.

Adobe Flash Player for Linux:

Update to version 11.2.202.451.

Adobe AIR Desktop runtime, AIR SDK, AIR SDK & Compiler, and AIR Android:

Update to version 17.0.0.144.

Credits:

5, 6)	Natalie Silvanovich, Google Project Zero
9)	Reported by the vendor.
10)	bilou via ZDI

The vendor credits:

1, 3)	Chris Evans, Google Project Zero
2)	Yuki Chen and Xiaoning Li, Intel Labs and Haifei Li, McAfee Labs
4)	Mark Brand, Google Project Zero
7, 8)	Soroush Dalili, NCC Group
11)	Jihui Lu, KeenTeam via Chromium vulnerability reward program

Changelog:

2015-04-17: Added “Adobe AIR 17.x” to the list of affected products due to an update of the vendor’s advisory. Updated “Description” and “Solution” sections concerning Adobe AIR products. Updated title.
2015-05-07: Updated vulnerabilities #5 and #6 with additional details. Updated credits. Added links to the “Original Advisory” section.

Original Advisory:

Adobe: https://helpx.adobe.com/security/products/flash-player/apsb15-05.html

ZDI: http://www.zerodayinitiative.com/advisories/ZDI-15-087/

Google Project Zero:

http://googleprojectzero.blogspot.dk/2015/04/a-tale-of-two-exploits.html
https://code.google.com/p/google-security-research/issues/detail?id=229
https://code.google.com/p/google-security-research/issues/detail?id=260

References

SAID References: https://vim4.secunia.com?action=viewadvisory&vulnid=62621