



CVE-2013-6774

Published on: 03/30/2014 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:38 PM UTC

CVE-2013-6774

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



Certain versions of [Chainsdd Superuser](#) from [Androidsu](#) contain the following vulnerability:

Untrusted search path vulnerability in the ChainsDD Superuser package 3.1.3 for Android 4.2.x and earlier, CyanogenMod/ClockWorkMod/Koush Superuser package 1.0.2.1 for Android 4.2.x and earlier, and Chainfire SuperSU package before 1.69 for Android 4.2.x and earlier allows attackers to load an arbitrary .jar file

and gain privileges via a crafted BOOTCLASSPATH environment variable for a /system/xbin/su process. NOTE: another researcher was unable to reproduce this with ChainsDD Superuser.

CVE-2013-6774 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **10 - HIGH**

Access
Vector

NETWORK

Access
Complexity

LOW

Authentication

NONE

Confidentiality
Impact

COMPLETE

Integrity
Impact

COMPLETE

Availability
Impact

COMPLETE

CVE References

Description

Tags

Link

SecurityFocus

[Exploit](#)

www.securityfocus.com

[text/html](#)

[BUGTRAQ 20131113 Superuser unsanitized environment vulnerability on Android <= 4.2.x](#)

SecurityFocus

www.securityfocus.com

[text/html](#)

[BUGTRAQ 20131114 Re: Superuser unsanitized environment vulnerability on Android <= 4.2.x](#)

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not warrant the accuracy or completeness of the information provided on these sites. CVEreport is not responsible for any damage or loss resulting from the use of the information provided on these sites.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)						
Type	Vendor	Product	Version	Update	Edition	Language
Application	Androidsu	Chainsdd Superuser	3.1.3	All	All	All
Application	Androidsu	Chainsdd Superuser	3.1.3	All	All	All
Application	Chainfire	Supersu	1.69	All	All	All
Application	Chainfire	Supersu	1.69	All	All	All
Operating System	Google	Android	1.0	All	All	All
Operating System	Google	Android	1.1	All	All	All
Operating System	Google	Android	1.5	All	All	All
Operating System	Google	Android	1.6	All	All	All
Operating System	Google	Android	2.0	All	All	All
Operating System	Google	Android	2.0.1	All	All	All
Operating System	Google	Android	2.1	All	All	All
Operating System	Google	Android	2.2	All	All	All
Operating System	Google	Android	2.2	rev1	All	All
Operating System	Google	Android	2.2.1	All	All	All
Operating System	Google	Android	2.2.2	All	All	All
Operating System	Google	Android	2.2.3	All	All	All
Operating System	Google	Android	2.3	All	All	All
Operating System	Google	Android	2.3	rev1	All	All
Operating System	Google	Android	2.3.1	All	All	All
Operating System	Google	Android	2.3.2	All	All	All
Operating System	Google	Android	2.3.3	All	All	All

System						
Operating System	Google	Android	2.3.4	All	All	All
Operating System	Google	Android	2.3.5	All	All	All
Operating System	Google	Android	2.3.6	All	All	All
Operating System	Google	Android	2.3.7	All	All	All
Operating System	Google	Android	3.0	All	All	All
Operating System	Google	Android	3.1	All	All	All
Operating System	Google	Android	3.2	All	All	All
Operating System	Google	Android	3.2.1	All	All	All
Operating System	Google	Android	3.2.2	All	All	All
Operating System	Google	Android	3.2.4	All	All	All
Operating System	Google	Android	3.2.6	All	All	All
Operating System	Google	Android	4.0	All	All	All
Operating System	Google	Android	4.0.1	All	All	All
Operating System	Google	Android	4.0.2	All	All	All
Operating System	Google	Android	4.0.3	All	All	All
Operating System	Google	Android	4.0.4	All	All	All
Operating System	Google	Android	4.1	All	All	All
Operating System	Google	Android	4.1.2	All	All	All
Operating System	Google	Android	4.2	All	All	All
Operating System	Google	Android	4.2.1	All	All	All
Operating System	Google	Android	4.2.2	All	All	All
Operating System	Google	Android	1.0	All	All	All
Operating System	Google	Android	1.1	All	All	All

System						
Operating System	Google	Android	1.5	All	All	All
Operating System	Google	Android	1.6	All	All	All
Operating System	Google	Android	2.0	All	All	All
Operating System	Google	Android	2.0.1	All	All	All
Operating System	Google	Android	2.1	All	All	All
Operating System	Google	Android	2.2	All	All	All
Operating System	Google	Android	2.2	rev1	All	All
Operating System	Google	Android	2.2.1	All	All	All
Operating System	Google	Android	2.2.2	All	All	All
Operating System	Google	Android	2.2.3	All	All	All
Operating System	Google	Android	2.3	All	All	All
Operating System	Google	Android	2.3	rev1	All	All
Operating System	Google	Android	2.3.1	All	All	All
Operating System	Google	Android	2.3.2	All	All	All
Operating System	Google	Android	2.3.3	All	All	All
Operating System	Google	Android	2.3.4	All	All	All
Operating System	Google	Android	2.3.5	All	All	All
Operating System	Google	Android	2.3.6	All	All	All
Operating System	Google	Android	2.3.7	All	All	All
Operating System	Google	Android	3.0	All	All	All
Operating System	Google	Android	3.1	All	All	All
Operating System	Google	Android	3.2	All	All	All
Operating	Google	Android	3.2.1	All	All	All

System						
Operating System	Google	Android	3.2.2	All	All	All
Operating System	Google	Android	3.2.4	All	All	All
Operating System	Google	Android	3.2.6	All	All	All
Operating System	Google	Android	4.0	All	All	All
Operating System	Google	Android	4.0.1	All	All	All
Operating System	Google	Android	4.0.2	All	All	All
Operating System	Google	Android	4.0.3	All	All	All
Operating System	Google	Android	4.0.4	All	All	All
Operating System	Google	Android	4.1	All	All	All
Operating System	Google	Android	4.1.2	All	All	All
Operating System	Google	Android	4.2	All	All	All
Operating System	Google	Android	4.2.1	All	All	All
Operating System	Google	Android	4.2.2	All	All	All
Application	Koushik Dutta	Superuser	1.0.2.1	All	All	All
Application	Koushik Dutta	Superuser	1.0.2.1	All	All	All
cpe:2.3:a:androidsu:chainsdd_superuser:3.1.3:*:*:*:*:android:*:*:						
cpe:2.3:a:androidsu:chainsdd_superuser:3.1.3:*:*:*:*:android:*:*:						
cpe:2.3:a:chainfire:supersu:1.69:*:*:*:*:android:*:*:						
cpe:2.3:a:chainfire:supersu:1.69:*:*:*:*:android:*:*:						
cpe:2.3:o:google:android:1.0:*:*:*:*:*:*:						
cpe:2.3:o:google:android:1.1:*:*:*:*:*:*:						
cpe:2.3:o:google:android:1.5:*:*:*:*:*:*:						
cpe:2.3:o:google:android:1.6:*:*:*:*:*:*:						
cpe:2.3:o:google:android:2.0:*:*:*:*:*:*:						
cpe:2.3:o:google:android:2.0.1:*:*:*:*:*:*:						

cpe:2.3:o:google:android:2.1:*****:
cpe:2.3:o:google:android:2.2:*****:
cpe:2.3:o:google:android:2.2:rev1:*****:
cpe:2.3:o:google:android:2.2.1:*****:
cpe:2.3:o:google:android:2.2.2:*****:
cpe:2.3:o:google:android:2.2.3:*****:
cpe:2.3:o:google:android:2.3:*****:
cpe:2.3:o:google:android:2.3:rev1:*****:
cpe:2.3:o:google:android:2.3.1:*****:
cpe:2.3:o:google:android:2.3.2:*****:
cpe:2.3:o:google:android:2.3.3:*****:
cpe:2.3:o:google:android:2.3.4:*****:
cpe:2.3:o:google:android:2.3.5:*****:
cpe:2.3:o:google:android:2.3.6:*****:
cpe:2.3:o:google:android:2.3.7:*****:
cpe:2.3:o:google:android:3.0:*****:
cpe:2.3:o:google:android:3.1:*****:
cpe:2.3:o:google:android:3.2:*****:
cpe:2.3:o:google:android:3.2.1:*****:
cpe:2.3:o:google:android:3.2.2:*****:
cpe:2.3:o:google:android:3.2.4:*****:
cpe:2.3:o:google:android:3.2.6:*****:
cpe:2.3:o:google:android:4.0:*****:
cpe:2.3:o:google:android:4.0.1:*****:
cpe:2.3:o:google:android:4.0.2:*****:
cpe:2.3:o:google:android:4.0.3:*****:
cpe:2.3:o:google:android:4.0.4:*****:
cpe:2.3:o:google:android:4.1:*****:
cpe:2.3:o:google:android:4.1.2:*****:

cpe:2.3:o:google:android:4.1.*:*:*:*:*:
cpe:2.3:o:google:android:4.2.*:*:*:*:*:
cpe:2.3:o:google:android:4.2.1.*:*:*:*:*:
cpe:2.3:o:google:android:4.2.2.*:*:*:*:*:
cpe:2.3:o:google:android:1.0.*:*:*:*:*:
cpe:2.3:o:google:android:1.1.*:*:*:*:*:
cpe:2.3:o:google:android:1.5.*:*:*:*:*:
cpe:2.3:o:google:android:1.6.*:*:*:*:*:
cpe:2.3:o:google:android:2.0.*:*:*:*:*:
cpe:2.3:o:google:android:2.0.1.*:*:*:*:*:
cpe:2.3:o:google:android:2.1.*:*:*:*:*:
cpe:2.3:o:google:android:2.2.*:*:*:*:*:
cpe:2.3:o:google:android:2.2:rev1.*:*:*:*:*:
cpe:2.3:o:google:android:2.2.1.*:*:*:*:*:
cpe:2.3:o:google:android:2.2.2.*:*:*:*:*:
cpe:2.3:o:google:android:2.2.3.*:*:*:*:*:
cpe:2.3:o:google:android:2.3.*:*:*:*:*:
cpe:2.3:o:google:android:2.3:rev1.*:*:*:*:*:
cpe:2.3:o:google:android:2.3.1.*:*:*:*:*:
cpe:2.3:o:google:android:2.3.2.*:*:*:*:*:
cpe:2.3:o:google:android:2.3.3.*:*:*:*:*:
cpe:2.3:o:google:android:2.3.4.*:*:*:*:*:
cpe:2.3:o:google:android:2.3.5.*:*:*:*:*:
cpe:2.3:o:google:android:2.3.6.*:*:*:*:*:
cpe:2.3:o:google:android:2.3.7.*:*:*:*:*:
cpe:2.3:o:google:android:3.0.*:*:*:*:*:
cpe:2.3:o:google:android:3.1.*:*:*:*:*:
cpe:2.3:o:google:android:3.2.*:*:*:*:*:
cpe:2.3:o:google:android:3.2.1.*:*:*:*:*:

cpe:2.3:o:google:android:3.2.2:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:o:google:android:3.2.4:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:o:google:android:3.2.6:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:o:google:android:4.0:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:o:google:android:4.0.1:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:o:google:android:4.0.2:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:o:google:android:4.0.3:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:o:google:android:4.0.4:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:o:google:android:4.1:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:o:google:android:4.1.2:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:o:google:android:4.2:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:o:google:android:4.2.1:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:o:google:android:4.2.2:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:a:koushik_dutta:superuser:1.0.2.1:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:a:koushik_dutta:superuser:1.0.2.1:~::~~::~~::~~::~~::~~::~~:::

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID→](#)