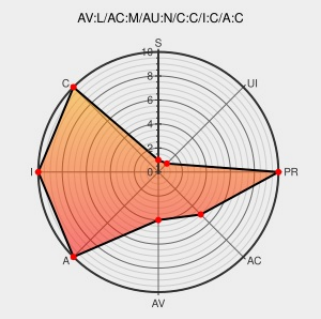
CVE-2014-1680

Published on: 02/13/2014 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:47 PM UTC

CVE-2014-1680

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Bandizip from Bandisoft contain the following vulnerability:

Untrusted search path vulnerability in Bandisoft Bandizip before 3.10 allows local users to gain privileges via a Trojan horse dwmapi.dll file in the current working directory.

CVE-2014-1680 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 6.9 - MEDIUM

Access Vector	Access Complexity	Authentication
LOCAL	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
Bandizip 3.09 DLL Hijack ≈ Packet Storm	Exploit, packetstormsecurity.com, text/html	MISC packetstormsecurity.com/files/125059
Bandizip - Download Free Zip Archiver to open ZIP, RAR, 7z files	www.bandisoft.com, text/html	MISC www.bandisoft.com/bandizip/history
No Description Provided	osvdb.org, Inactive Link, Not Archived	OSVDB 102979
IBM X-Force Exchange	exchange.xforce.ibmcloud.com, text/html	XF bandzip-dll-cve20141680-code-exec(90966)

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 endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Bandisoft	Bandizip	3.00	All	All	All
Application	Bandisoft	Bandizip	3.01	All	All	All
Application	Bandisoft	Bandizip	3.02	All	All	All
Application	Bandisoft	Bandizip	3.03	All	All	All
Application	Bandisoft	Bandizip	3.04	All	All	All
Application	Bandisoft	Bandizip	3.05	All	All	All
Application	Bandisoft	Bandizip	3.06	All	All	All
Application	Bandisoft	Bandizip	3.07	All	All	All
Application	Bandisoft	Bandizip	3.08	All	All	All
Application	Bandisoft	Bandizip	3.00	All	All	All
Application	Bandisoft	Bandizip	3.01	All	All	All
Application	Bandisoft	Bandizip	3.02	All	All	All
Application	Bandisoft	Bandizip	3.03	All	All	All
Application	Bandisoft	Bandizip	3.04	All	All	All
Application	Bandisoft	Bandizip	3.05	All	All	All
Application	Bandisoft	Bandizip	3.06	All	All	All
Application	Bandisoft	Bandizip	3.07	All	All	All
Application	Bandisoft	Bandizip	3.08	All	All	All
Application	Bandisoft	Bandizip	All	All	All	All

cpe:2.3:a:bandisoft:bandizip:3.00:*:*:*:*:*:*:*:

cpe:2.3:a:bandisoft:bandizip:3.01:*:*:*:*:*:*:*:

cpe:2.3:a:bandisoft:bandizip:3.02:*:*:*:*:*:*:*:

cpe:2.3:a:bandisoft:bandizip:3.03:*:*:*:*:*:*:*:

cpe:2.3:a:bandisoft:bandizip:3.04:*:*:*:*:*:*:*:

cpe:2.3:a:bandisoft:bandizip:3.05:*:*:*:*:*:*:*:

cpe:2.3:a:bandisoft:bandizip:3.06:*:*:*:*:*:*:*:

cpe:2.3:a:bandisoft:bandizip:3.07:*:*:*:*:*:*:*:

cpe:2.3:a:bandisoft:bandizip:3.08:*:*:*:*:*:*:*:

cpe:2.3:a:bandisoft:bandizip:3.00:*:*:*:*:*:*:*:

cpe:2.3:a:bandisoft:bandizip:3.01:*:*:*:*:*:*:*:

cpe:2.3:a:bandisoft:bandizip:3.02:*:*:*:*:*:*:*:

cpe:2.3:a:bandisoft:bandizip:3.03:*:*:*:*:*:*:*:

cpe:2.3:a:bandisoft:bandizip:3.04:*:*:*:*:*:*:*:

cpe:2.3:a:bandisoft:bandizip:3.05:*:*:*:*:*:*:*:

cpe:2.3:a:bandisoft:bandizip:3.06:*:*:*:*:*:*:*:

cpe:2.3:a:bandisoft:bandizip:3.07:*:*:*:*:*:*:*:

cpe:2.3:a:bandisoft:bandizip:3.08:*:*:*:*:*:*:*:

cpe:2.3:a:bandisoft:bandizip:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→