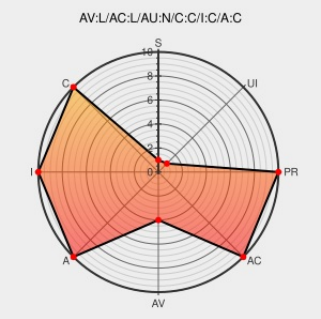
CVE-2004-1649

Published on: 08/31/2004 04:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:10 PM UTC

CVE-2004-1649

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



Certain versions of Windows 2000 from Microsoft contain the following vulnerability:

Buffer overflow in Microsoft Msinfo32.exe might allow local users to execute arbitrary code via a long filename in the msinfo_file command line parameter. NOTE: this issue might not cross security boundaries, so it may be REJECTED in the future.

CVE-2004-1649 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 7.2 - HIGH

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

CVE References

Description	Tags	Link
IBM X-Force Exchange	exchange.xforce.ibmcloud.com, text/html	XF msinfo-msinfofile-bo(17153)
'RE: [Full-Disclosure] MSInfo Buffer Overflow' - MARC	marc.info, text/html	FULLDISC 20040830 MSInfo Buffer Overflow
'MSInfo Buffer Overflow' - MARC	marc.info, text/html	BUGTRAQ 20040831 MSInfo Buffer Overflow
[Full-Disclosure] MSInfo Buffer Overflow	Exploit, Vendor Advisory, web.archive.org, text/html, Inactive Link, Not Archived	FULLDISC 20040830 MSInfo Buffer Overflow

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
Operating System	Microsoft	Windows 2000	All	All	All	All
Operating System	Microsoft	Windows 2000	All	All	All	All

cpe:2.3:o:microsoft:windows_2000:*:*:*:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_2000:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→