



CVE-2004-0600

Published on: 07/23/2004 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:12 PM UTC

CVE-2004-0600

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Samba](#) from [Samba](#) contain the following vulnerability:

Buffer overflow in the Samba Web Administration Tool (SWAT) in Samba 3.0.2 to 3.0.4 allows remote attackers to execute arbitrary code via an invalid base-64 character during HTTP basic authentication.

CVE-2004-0600 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

Home - Conectiva

[distro.conectiva.com.br](#)
[text/html](#)

[CONECTIVA CLA-2004:851](#)

'Security Release - Samba 3.0.5 and 2.2.10' - MARC

[marc.info](#)
[text/html](#)

[BUGTRAQ 20040722 Security Release - Samba 3.0.5 and 2.2.10](#)

Repository / Oval Repository

[oval.cisecurity.org](#)
[text/html](#)

[OVAL oval:org.mitre.oval:def:11445](#)

'Samba 3.x swat preauthentication buffer overflow' - MARC

[marc.info](#)
[text/html](#)

[BUGTRAQ 20040722 Samba 3.x swat preauthentication buffer overflow](#)

redhat.com | Red Hat Support

[Patch](#)
[Vendor Advisory](#)
[www.redhat.com](#)
[text/html](#)

[REDHAT RHSA-2004:259](#)

Gentoo Linux Documentation -- Samba: Multiple buffer overflows	www.gentoo.org text/html	 GENTOO GLSA-200407-21
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	 XF samba-swat-base64-bo(16785)
'[OpenPKG-SA-2004.033] OpenPKG Security Advisory (samba)' - MARC	marc.info text/html	 BUGTRAQ 20040722 [OpenPKG-SA-2004.033] OpenPKG Security Advisory (samba)
'SWAT PreAuthorization PoC' - MARC	marc.info text/html	 BUGTRAQ 20040722 SWAT PreAuthorization PoC
	www.trustix.org text/plain Inactive Link Not Archived	 TRUSTIX 2004-0039
'TSSA-2004-014 - samba' - MARC	marc.info text/html	 BUGTRAQ 20040722 TSSA-2004-014 - samba
Home - Conectiva	distro.conectiva.com.br text/html	 CONECTIVA CLA-2004:854
No Description Provided	www.mandrakesecure.net Inactive Link Not Archived	 MANDRAKE MDKSA-2004:071
Security Announcement	web.archive.org text/html Inactive Link Not Archived	 SUSE SUSE-SA:2004:022

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	Samba	Samba	3.0.2	All	All	All
Application	Samba	Samba	3.0.2a	All	All	All
Application	Samba	Samba	3.0.3	All	All	All
Application	Samba	Samba	3.0.4	All	All	All
Application	Samba	Samba	3.0.2	All	All	All
Application	Samba	Samba	3.0.2a	All	All	All
Application	Samba	Samba	3.0.3	All	All	All
Application	Samba	Samba	3.0.4	All	All	All
Operating System	Trustix	Secure Linux	1.5	All	All	All
Operating System	Trustix	Secure Linux	2.0	All	All	All
Operating System	Trustix	Secure Linux	2.1	All	All	All

Operating System	Trustix	Secure Linux	1.5	All	All	All
Operating System	Trustix	Secure Linux	2.0	All	All	All
Operating System	Trustix	Secure Linux	2.1	All	All	All
cpe:2.3:a:samba:samba:3.0.2:*:*:*:*:*:						
cpe:2.3:a:samba:samba:3.0.2a:*:*:*:*:*:						
cpe:2.3:a:samba:samba:3.0.3:*:*:*:*:*:						
cpe:2.3:a:samba:samba:3.0.4:*:*:*:*:*:						
cpe:2.3:a:samba:samba:3.0.2:*:*:*:*:*:						
cpe:2.3:a:samba:samba:3.0.2a:*:*:*:*:*:						
cpe:2.3:a:samba:samba:3.0.3:*:*:*:*:*:						
cpe:2.3:a:samba:samba:3.0.4:*:*:*:*:*:						
cpe:2.3:o:trustix:secure_linux:1.5:*:*:*:*:*:						
cpe:2.3:o:trustix:secure_linux:2.0:*:*:*:*:*:						
cpe:2.3:o:trustix:secure_linux:2.1:*:*:*:*:*:						
cpe:2.3:o:trustix:secure_linux:1.5:*:*:*:*:*:						
cpe:2.3:o:trustix:secure_linux:2.0:*:*:*:*:*:						
cpe:2.3:o:trustix:secure_linux:2.1:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

[← Previous ID](#)

Next ID→

© CVE.report 2023 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status status.cve.report