# [SECURITY] [DSA 5205-1] samba security update

Article URL
www.securityhome.eu/mailings/mailing.php?mid=21235

Author
SecurityHome.eu

Published: 11 August 2022

- -------------------------------------------------------------------------
Debian Security Advisory DSA-5205-1 security@debian.org
https://www.debian.org/security/ Salvatore Bonaccorso
August 11, 2022 https://www.debian.org/security/faq
- -------------------------------------------------------------------------

Package : samba
CVE ID : CVE-2022-2031 CVE-2022-32742 CVE-2022-32744 CVE-2022-32745
CVE-2022-32746
Debian Bug : 1016449

Several vulnerabilities have been discovered in Samba, a SMB/CIFS file,
print, and login server for Unix.

CVE-2022-2031

Luke Howard reported that Samba AD users can bypass certain
restrictions associated with changing passwords. A user who has been
requested to change their password can exploit this to obtain and
use tickets to other services.

CVE-2022-32742

Luca Moro reported that a SMB1 client with write access to a share
can cause server memory content to be leaked.

CVE-2022-32744

Joseph Sutton reported that Samba AD users can forge password change
requests for any user, resulting in privilege escalation.

CVE-2022-32745

Joseph Sutton reported that Samba AD users can crash the server process with a specially crafted LDAP add or modify request.

CVE-2022-32746

Joseph Sutton and Andrew Bartlett reported that Samba AD users can cause a use-after-free in the server process with a specially crafted LDAP add or modify request.

For the stable distribution (bullseye), these problems have been fixed in version 2:4.13.13+dfsg-1~deb11u5. The fix for CVE-2022-32745 required an update to ldb 2:2.2.3-2~deb11u2 to correct the defect.

We recommend that you upgrade your samba packages.

For the detailed security status of samba please refer to its security tracker page at:
https://security-tracker.debian.org/tracker/samba

Further information about Debian Security Advisories, how to apply these updates to your system and frequently asked questions can be found at: https://www.debian.org/security/

Mailing list: debian-security-announce@lists.debian.org