VULNERABILITY BULLETINS

New Samba Bug Allows Remote Attackers to Execute Arbitrary Code as Root

○○○ TLP:WHITE

Feb 04, 2022

Health-ISAC is issuing a vulnerability bulletin regarding multiple security vulnerabilities in the Windows/Linux interoperability suite Samba that if exploited, could allow remote attackers to execute arbitrary code with the highest privileges on affected installations.

Samba has since issued software updates to address these vulnerabilities, which concern an out-of-bounds heap read-write vulnerability, allowing remote attackers to execute arbitrary code as root on affected Samba installations that use the virtual file system (VFS) module vfs_fruit. Installing the latest Samba security updates is highly recommended, and can be accessed here.

More information on the vulnerabilities has been included further in this vulnerability bulletin for your security awareness.

Samba is an interoperability suite that allows Windows and Linus/Unix-based hosts to work together and share file and print services with multi-platform devices on a common network, including Server Message Block (SMB) file-sharing.

The chief flaw among these security vulnerabilities for Samba is CVE-2021-44142, which impacts all versions of Samba before 4.13.17 and concerns an out-of-bounds heap read/write vulnerability in the VFS module, vfs_fruit, which provides compatibility with Apple server message block clients.

The flaws also affect widely used Linux distributions such as Red Hat, SUSE Linux, and Ubuntu. The specific flaw exists within the parsing of metadata in the Samba server daemon when opening a file. An attacker can leverage this vulnerability to execute code in the context of root.

Two other flaws were also addressed in the latest update, CVE-2021-44141, which concerns an information leak via symlinks of the existence of files or directories outside of the exported share; and CVE-2022-0336, in which Samba AD users with permission to write into an account can impersonate arbitrary services.

More information on these vulnerabilities can be found here and here.

Reference(s)	Samba, Zero Day Initiative, Samba, Samba, Samba, The Hacker News

CVE(s)
CVE-2021-44142

CVE-2021-44141

CVE-2022-0336

Recommendations
Samba 4.13.17, 4.14.12, and 4.15.5 are the latest patched versions; administrators are urged to upgrade to these releases as soon as possible.

Two workarounds can also be employed in case updating to the latest versions is not feasible.

1. Administrators can remove the fruit *module* from the list of VFS objects in Samba configuration files.
2. Administrators could also conceivably change the default settings for the *fruit:metadata* or *fruit:resource* modules, but Samba warned that this would cause all stored information to be inaccessible and will make it appear to macOS clients as if the information is lost.

Release Date
Feb 04, 2022

Sources
Samba: Security Releases

Samba: More Information on CVE-2021-44142

Samba: More Information on CVE-2021-44141

Samba: More Information on CVE-2022-0336

Zero Day Initiative: Details on a Samba Code Execution Bug Demonstrated at PWN2OWN Austin

The Hacker News: New Samba Bug Allows Remote Attackers to Execute Arbitrary Code as Root

Alert ID a88b4f3f

View Alert

Tags Samba cifs-utils, Vulnerability Bulletin, Vulnerability, Samba Active Directory Domain Controller, Samba Software, Samba 4.10.5, Samba 4.9.9, Samba

TLP:WHITE Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

For Questions or Comments Please email us at toc@h-isac.org