Impactful vulnerabilities detected nginx [CVE-2001-0641_COPY,CVE-2001-0644_COPY]

Overview

nginx is vulnerable to ...
An attacker can use it to ...

The CTI team at Leonardo has detected the following vulnerabilities CVE-2001-0641_COPY and CVE-2001-0644_COPY.

Description

Nginx is a multifunctional web server with a broad range of applications, including serving as a reverse proxy, load balancer, mail proxy, and HTTP cache. It was designed by Igor Sysoev and made available to the public in 2004 as an open-source software operating under the 2-clause BSD license. Its popularity among web servers is extraordinarily high, especially as a load balancer. According to security experts, Nginx has been operational since April 15, 2020, serving as a reconnaissance tool for various functions.

On 12 April 2023, 2 vulnerabilities have been disclosed.

Cve-2001-0641_copy represents a concerning vulnerability for Linux users. The security flaw stems from a buffer overflow in the man program across multiple Linux distributions. It grants local users the ability to execute malicious code under the guise of group man, simply by utilizing a lengthy -S option. With a cvss score of 4.0 and an exploitability score of 5.0, the impact score of Cve-2001-0641_copy is also rated at 4.0. This vulnerability is currently present in Linux products, including Ubuntu and Debian.

Cve-2001-0644_copy is a significant vulnerability that impacts Maxum Rumpus FTP Server 1.3.3 and 2.0.3 dev 3. The security flaw involves the storage of passwords in plaintext within the "Rumpus User Database" file in the prefs folder. This flaw creates an opportunity for attackers to gain server privileges. The vulnerability's CVSS score is high, at 7.0, with an exploitability score of 6.0 and an impact score of 6.0. The flaw is present in Microhard products, specifically the WindowHash product. Immediate attention is warranted to address this security concern.

The table below includes further details about the vulnerabilities, including the product affected by the security flaw, vendor, CVSSv2 and CVSSv3 score.

ID	CVSSv2	CVSSv3	Vendor	Products	Name
CVE-2001-0641_COPY	4.0	3.8	Linux	Ubuntu and Debian	CVE-2001-0641_COPY
CVE-2001-0644_COPY	7.0	7.0	Microhard	WindowHash	CVE-2001-0644_COPY

Mitigations

Recommended Actions

In line with the CISA guidelines, and following the instructions of the relevant vendor, it is advisable, where possible, to install the latest security updates for products affected by the above vulnerabilities. It is also advisable to prioritize the patching of vulnerabilities affecting services exposed on the Internet and then those with higher CVSS scores.

Appendix 1

CVE-2001-0641_COPY CVSS 3.0: 3.8
Vulnerability Description: Buffer overflow in man program in various distributions of Linux allows local user to execute arbitrary code as group man via a long -S option.
Recommended Mitigations: Restrict Registry Permissions and Restrict File and Directory Permissions
Detection Methods: List of detection methods
Vulnerable Configurations: None

CVSS3					
Base	3.8	Impact	4.0	Exploitability	3.8
Access	Attack Complexity	Attack vector	Privileges Required	Scope	User Interaction
	Low	Adjacent	Low	changed	None
Impact	Confidentiality		Integrity	Availability	
	High		High	None	

Source

None

Appendix 2

CVE-2001-0644_COPY CVSS 3.0: 7.0
Vulnerability Description: Maxum Rumpus FTP Server 1.3.3 and 2.0.3 dev 3 stores passwords in plaintext in the "Rumpus User Database" file in the prefs folder, which could allow attackers to gain privileges on the server.
Recommended Mitigations: User Training
Detection Methods: List of detection methods
Vulnerable Configurations: None

CVSS3					
Base	7.0	Impact	5.8	Exploitability	7.0
Access	Attack Complexity	Attack vector	Privileges Required	Scope	User Interaction
	High	Network	High	unchanged	Required
Impact	Confidentiality		Integrity	Availability	
	High		Low	Low	

Source

https://en.wikipedia.org/wiki/Nginx