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 an infrastructure. The description of the infrastructure is: Nginx is a web server that can also be used as a reverse proxy, load balancer, mail proxy and HTTP cache. The software was created by Igor Sysoev and publicly released in 2004. Nginx is free and open-source software, released under the terms of the 2-clause BSD license. A large fraction of web servers use Nginx, often as a load balancer. According to security researchers, the infrastructure has been active since 15 April 2020. It type is reconnaissance.

On 12 April 2023, 2 vulnerabilities have been disclosed.

Cve-2001-0641_copy is a vulnerability. The description of the security flaw is: 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. The vulnerability cvss score is 4.0. It exploitability score is 5.0. Cve-2001-0641_copy impact score is 4.0. It is present in products offered by Linux. The security flaw affects these products Ubuntu and Debian.

Cve-2001-0644_copy is a vulnerability. The description of the security flaw is: 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. It cvss score is 7.0. Cve-2001-0644_copy exploitability score is 6.0. It impact score is 6.0. The security flaw is present in products offered by Microhard. The vulnerability affects this product WindowHash.

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