Mphasis
The Next Applied

Mphasis SOC – Information Security News
Date & Time Issued: 05-JUL-2024, 20:30 IST

Title	**Critical HTTP File Server Vulnerability (CVE-2024-23692) Actively Exploited to Deploy Cryptomining Malware, RATs, Stealers**
Summary	• HTTP File Server (HFS) is a program that provides a simple type of web service. Because it can provide web services with just an executable file without having to build a web server, it is often used for sharing files, allowing users to connect to the address through web browsers and easily download files. • A remote code execution vulnerability (CVE-2024-23692) in HFS was announced. Using this, the threat actor can send packets containing commands to HFS and have it execute malicious commands. Although not the latest version, the vulnerability affects "HFS 2.3m" which is used by many users.
Severity	Medium
Attack Vectors	• Using this, one can send packets containing commands to HFS servers remotely as shown below. This means that the threat actor can exploit the CVE-2024-23692 vulnerability after scanning the externally exposed HFS service to install malware or obtain control. • After initial infiltration, the threat actors used commands such as "whoami" or "arp" to collect information on the system. They then added backdoor accounts to connect via RDP and concealed the Accounts. In many cases, HFS was terminated after the process was complete so that it would not be used by other threat actors. • XMRig, a CoinMiner that mines the Monero cryptocurrency, was the one the most used in the attacks. At least 4 threat actors are attacking HFS and installing CoinMiners. LemonDuck is a known threat actor out of those attackers • Out of the malware strains used in the attack, PlugX is a variant of the BackDoor.PlugX. PlugX Malware Being Distributed via Vulnerability Exploitation." A small difference is that only the commands up to "0xA" are supported. In addition, "Disk", "Nethood", "Netstat", "Option", "PortMap", "Process", "RegEdit", "Service", "Shell", "SQL", and "Telnet" plugins are supported while "KeyLog", "Screen", "ClipLog", and "RDP" are excluded. • A major example is GoThief which uses Amazon AWS to steal information from the infected system. Developed in the Go language, AhnLab categorizes it under GoThief based on the source code path used for malware creation.

Indicator of Compromise	INDICATOR TYPE	INDICATORS
	File Hash	• Ce7dc5df5568a79affa540aa86b24773 • 8f0071027d513867feb3eb8943ccaf05 • 77970a04551636cc409e90d39bbea931 • 6adaeb6543955559c05a9de8f92d1e1d • 4383b1ea54a59d27e5e6b3122b3dadb2
	URL	• hxxp://121.204.249[.]123/2345.exe • hxxp://121.204.249[.]123:8077/systeminfo.exe • hxxp://185.173.93[.]167:13306/Roboform.dll • hxxp://185.173.93[.]167:13306/WindowsWatcher.key • hxxps://imgdev.s3.eu-west-3.amazonaws[.]com/dev/20210623/conost.exe • hxxp://188.116.22[.]65:5000/submit

Recommendations	• Block all identified IOCs at your security controls. • Limit Internet Access: Restrict internet access to your file servers. Only allow essential services (such as DNS and NTP) within your network to connect with the file servers. • Content Security Policy (CSP): Implement a Content Security Policy (CSP) with the frame-ancestors directive if possible. • SSL Certificate: Install an SSL certificate on your site. SSL encrypts information between parties, making it harder for attackers to intercept or manipulate data. • Employ multi-layered protection strategies to secure vulnerable assets effectively.
References	• https://asec.ahnlab.com/en/67650/ • https://socradar.io/critical-http-file-server-vulnerability-cve-2024-23692-actively-exploited-to-deploy-cryptomining-malware-rats-stealers/