Microsoft fixes 149 security vulnerabilities on Windows, users should update immediately

Microsoft just released an April security update to fix 149 security vulnerabilities on Windows, two of which are actively exploited in the wild.

Many security holes in Windows have just been patched

Of the 149 security vulnerabilities, 3 are rated severe, 142 are rated important, 3 are moderate, and 1 is rated low severity.

You can install the April security update by going to Start - Settings - Update and Security - Windows Update - Check for update. If any security updates are available, users just need to download and install them.

Two dangerous security vulnerabilities that are currently being actively exploited include:

1. - CVE-2024-26234 (CVSS score: 6.7) - Proxy driver spoofing vulnerability
2. - CVE-2024-29988 (CVSS score: 8.8) - Security feature bypass

Although Microsoft did not provide information about CVE-2024-26234, cybersecurity company Sophos said it discovered in December 2023 a malicious executable file ("Catalog.exe" or "Catalog Authentication Client"

Service") signed with a valid publisher certificate.

Analysis of the binary's authentication code revealed the publisher to be Hainan YouHu Technology, which also developed another tool called LaiXi Android Screen Mirroring.

The second software is described as "a marketing software. that can connect hundreds of mobile phones and control them in batches, while also automating tasks such as mass following, liking and comment."

Sophos researcher Andreas Klopsch said: 'We have no evidence that LaiXi developers intentionally embedded malicious files in their products, or that a threat actor conducted a supply chain attack. response to insert it into the compilation/build process of LaiXi' application.

The cybersecurity company said the vulnerability exploitation campaign has been underway since at least January 5, 2023.

Another security vulnerability believed to be actively exploited is CVE-2024-29988, which like CVE-2024-21412 and CVE-2023-36025, allows attackers to bypass SmartScreen protections. Microsoft Defender when opening a specially created file.

'To exploit this security feature bypass vulnerability, an attacker would need to persuade a user to launch malicious files using a launcher application that requires no user interface to be displayed,' Microsoft said.

Another important vulnerability is CVE-2024-29990 (CVSS score: 9.0), an elevation of privilege vulnerability affecting Microsoft Azure Kubernetes Service Confidential Containers. This vulnerability can be exploited by an unauthenticated attacker to steal authentication information.

Overall, Windows users should install the April security update as soon as possible as it addresses 68 remote code execution errors, 31 privilege escalation errors, 26 security feature bypass errors, and 6 denial of service (DoS) errors. Interestingly, 24 out of 26 security vulnerabilities are related to Secure Boot.

Satnam Narang, an engineer at Tenable said: 'While none of the Secure Boot vulnerabilities addressed this month were exploited in the wild, they serve as a reminder that vulnerabilities in Secure Boot still exists and we may see more malicious activities related to Secure Boot in the future'.

The revelation comes as Microsoft is facing criticism over its security practices, with a recent report from the US Cyber ??Security Review Board (CSRB) criticizing the company for did not do enough to stop a cyber espionage campaign by a Chinese threat actor tracked as Storm-0558.

In addition to Microsoft, security updates have also been released by other vendors in the past few weeks to fix a number of vulnerabilities, including:

1. - Adobe
2. - AMD
3. - Android
4. - Apache XML Security for C++
5. - Aruba Networks
6. - Atos
7. - Bosch
8. - Cisco
9. - D-Link

10. - Dell
11. - Drupal
12. - F5
13. - Fortinet
14. - Fortra
15. - GitLab
16. - Google Chrome
17. - Google Cloud
18. - Google Pixel
19. - Hikvision
20. - Hitachi Energy
21. - HP
22. - HP Enterprise
23. - HTTP/2
24. - IBM
25. - Ivanti
26. - Jenkins
27. - Lenovo
28. - LG webOS
29. - Linux distributions Debian, Oracle Linux, Red Hat, SUSE and Ubuntu
30. - MediaTek
31. - Mozilla Firefox, Firefox ESR and Thunderbird
32. - NETGEAR
33. - NVIDIA
34. - Qualcomm
35. - Rockwell Automation
36. - Rust
37. - Samsung
38. - SAP
39. - Schneider Electric
40. - Siemens
41. - Splunk
42. - Synology
43. - VMware
44. - WordPress
45. - Zoom