Security Newsletter

22 Apr 2024

Subscribe to this newsletter

GitHub comments abused to push malware via Microsoft repo URLs

A GitHub flaw, or possibly a design decision, is being abused by threat actors to distribute malware using URLs associated with Microsoft repositories, making the files appear trustworthy.

While most of the malware activity has been based around the Microsoft GitHub URLs, this "flaw" could be abused with any public repository on GitHub, allowing threat actors to create very convincing lures.

Yesterday, McAfee released a report on a new LUA malware loader distributed through what appeared to be a legitimate Microsoft GitHub repositories for the "C++ Library Manager for Windows, Linux, and MacOS," known as vcpkg, and the STL library.

Read More

More #News

- Fake cheat lures gamers into spreading infostealer malware
- 22,500 Palo Alto firewalls "possibly vulnerable" to ongoing attacks
- Cybercriminals pose as LastPass staff to hack password vaults

#Breach Log

- Russian Sandworm hackers targeted 20 critical orgs in Ukraine
- GitLab affected by GitHub-style CDN flaw allowing malware hosting
- Synlab Italia suspends operations following ransomware attack

#Patch Time!

- Exploit released for Palo Alto PAN-OS bug used in attacks, patch now
- Ivanti warns of critical flaws in its Avalanche MDM solution
- CrushFTP warns users to patch exploited zero-day “immediately”

#Tech and #Tools

- Microsoft will limit Exchange Online bulk emails to fight spam
- Critical Forminator plugin flaw impacts over 300k WordPress sites
- HelloKitty ransomware rebrands, releases CD Projekt and Cisco data

This content was created by Kindred Group Security. Please share if you enjoyed!

Kindred Group in brief

Kindred Group is one of the world's leading online gambling operators with business across Europe, US and Australia, offering more than 30 million customers across 9 brands a great form of entertainment in a safe, fair and sustainable environment. The company, which employs about 2,000 people, is listed on Nasdaq Stockholm Large Cap and is a member of the European Gaming and Betting Association (EGBA) and founding member of IBIA (Sports Betting Integrity Association). Kindred Group is audited and certified by eCOGRA for compliance with the 2014 EU Recommendation on Consumer Protection and Responsible Gambling (2014/478/EU). Read more on www.kindredgroup.com.

You can access the previous newsletters at https://news.infosecgur.us