SECRETCRAFT

SECRET NEWS

SAMSTAG, 10. JUNI 2023 Ausgabe # 23-23

Sicherheitslücke

Minecraft: Sicherheitslücke bei CurseForge & Bukkit

Was ist passiert?
Aufgrund von Berichten, die CurseForge erhalten hat, wurde festgestellt, dass ein böswilliger Nutzer mehrere Konten erstellt und Projekte mit Malware auf die Plattform hochgeladen hat. CF hat daraufhin alle Konten, die damit in Verbindung stehen, gesperrt.

In Zusammenarbeit mit der Autoren-Community hat das CurseForge-Team eine gründliche Untersuchung durchgeführt, um dieses Problem umgehend zu lösen und sicherzustellen, dass solche bösartigen Handlungen in Zukunft verhindert werden. Das Hauptziel von CF ist es, eine schnelle Lösung zu finden und Präventivmaßnahmen zu ergreifen.

Hier erfahrt ihr, wie ihr ein Detektor-Tool verwenden könnt, mit dem ihr feststellen könnt, ob euer Computer infiziert wurde.

Woran erkenne ich, ob ich infiziert bin, und was kann ich tun?
Schaut euch zunächst die Liste der Projekte am Ende dieses Artikels an. Wenn ihr wisst, dass ihr keines dieser Projekte im letzten Monat heruntergeladen habt, solltet ihr laut CF sicher sein.

Beachtet auch, dass diese Malware nur PC und Linux infiziert, nicht aber Mac.
Wenn ihr euch jedoch nicht sicher seid oder euch vergewissern möchtet, könnt ihr mit den nachfolgenden Schritten weiter machen.

Es gibt 2 Schritte, mit denen ihr sicherstellen könnt, dass ihr sicher seid:

Feststellen, ob euer PC bereits infiziert ist
1. Ladet das Erkennungstool von hier (Windows) oder hier (Linux) herunter und führt es aus. Das GitHub-Projekt findet ihr hier.
Mit diesem Tool könnt ihr überprüfen, ob euer PC infiziert ist. Das Tool liefert eine Liste der Dateien, die auf eurem PC gefunden wurden.

2. Wenn ihr das Erkennungsprogramm ausgeführt habt und eine Infektion festgestellt wurde, stellt zunächst sicher, dass euch auch versteckte Dateien angezeigt werden.
Geht dazu unter Windows einfach zum oberen Rand des Datei-Explorer- und klickt auf „Ansicht“ > „Ausgeblendete Objekte“.

3. Geht dann zu jedem Dateiziel und löscht diese Dateien.
Löscht den Ordner „Microsoft Edge“ (mit Leerzeichen) vollständig. Der normale Edge-Ordner enthält kein Leerzeichen im Namen. Diese Malware erstellt speziell einen Ordner mit einem Leerzeichen darin.

Zusätzlich zu den oben genannten Schritten empfiehlt CF, bei einem Befall unabhängige Malware-Scanner auszuführen und alle wichtigen Kennwörter zu ändern.

Ermittelt, ob ihr ruhende/andere infizierte Mods/Jar-Dateien habt
1. Nachdem ihr den vorherigen Schritt abgeschlossen habt, führt das Jar-Malware-Scanning- Tool aus, um sicher zu gehen, dass eure anderen Mods, die nicht in der Liste unten aufgeführt sind, nicht infiziert sind. Dieses Tool sucht nach Stufe 0-Schwachstellen und ist in der Lage, alle infizierten Jars zu erkennen.
Führt das hier verlinkte Tool aus. Vollständiges Github hier.
2. Führt dieses Tool auch dann aus, wenn ihr in Schritt 1 als nicht infiziert eingestuft wurdet.

Verwendet das Tool, um alle Ordner zu scannen, die auf eurem PC installierte Minecraft Mod-Jars enthalten.

Klickt auf „Durchsuchen“ und wählt einen Ordner, der Jar-Dateien enthält, und klickt dann auf „Scannen“. Dadurch werden der ausgewählte Ordner und alle seine Unterordner überprüft.

Wenn eine infizierte Datei gefunden wurde, wird eine Meldung angezeigt. In diesem Fall löscht die Jar-Datei.
Stellt sicher, dass ihr alle Ordner auf eurem PC checkt, die Mods/Packs enthalten.

Live-Liste der bestätigten Mods, die infiziert wurden (Zuletzt aktualisiert - 06/08/2023 09:34 UTC)

Projekte, die infiziert waren und nun behoben sind:
Die meisten Projekte von LunaPixelStudios - Es ist ratsam, sicherzustellen, dass ihr die neueste Version eines Modpacks haben, da die notwendigen Korrekturen für diese Modpacks bereits verfügbar sein sollten und die infizierten Dateien gelöscht wurden:

- Buried Barrels
- Sky Villages [Forge/Fabric]
- Simply Houses
- When Dungeons Arise -Forge/Fabric
- Skyblock Core
- Prominence [FORGE]
- Medieval MC [FORGE] - MMC3
- Better MC [FORGE] - BMC3

Projekte, die infiziert sind und dauerhaft abgeschaltet werden:
1. Golem Awakening
2. Phanerozoic Worlds
3. Autobroadcast
4. Museum Curator Advanced
5. Vault Integrations (Bug Fix) **Note - Not the Modpack Vault Integrations*
6. AmazingTitles
7. dungeonx ** Note - Not DungeonZ*
8. HavenElytra
9. DisplayEntityEditor
10. The Nexus Event Custom Event
11. SimpleHarvesting
12. McBounties
13. More and Ore advanced
14. Easy Custom Foods
15. AntiCommandSpam Bungeecord Support
16. UltimateLevels
17. AntiRedstoneCrash
18. hydrationPlugin
19. NoVPN
20. Fragment Permission Plugin
21. Anti ChatReport
22. Additional Weapons+
23. UVision ENHANCED(server pack only)
24. UVision Server(server pack only)
25. UVision LITE (server pack only)
26. Create: Diesel and Oil Generators
27. Ultra Swords Mod
28. Simple Frames
29. AntiCrashXXL
30. Skelegram - The Skript Telegram Addon!

Quelle: CurseForge

ChangeLog

Das Joinen mit der neusten Bedrock Version (v1.20.0) ist nun möglich.
Ihr könnt den Server nun auch mit der 1.20 Java Version betreten, jedoch läuft der Server wie gehabt auf der 1.19.2 deswegen empfehlen wir weiterhin die 1.19.2 zu nutzen.

Event-Vorschau

Eure Kreativität ist wieder gefragt. Mit **/warp Event_Bauen** kommt ihr dort hin.