

Components:

Description:

Discord-Bot-Framework-Kernel is a Discord bot framework built with interactions.py, featuring modular extension management and secure execution. Because of the nature of arbitrary user-submitted code execution, this allows user to execute potentially malicious code to perform damage or extract sensitive information. By loading the module containing the following code and run the command, the bot token can be extracted. Then the attacker can load a blocking module to sabotage the bot (DDoS attack) and the token can be used to make the fake bot act as the real one. If the bot has very high privilege, the attacker basically has full control before the user kicks the bot. Any Discord user that hosts Discord-Bot-Framework-Kernel before commit f0d9e70841a0e3170b88c4f8d562018ccd8e8b14 is affected. Users are advised to upgrade. Users unable to upgrade may attempt to limit their discord bot's access via configuration options.

Main problems:

200 no CWE Description available