- DISCLOSED VULNERABILITY REPORT -

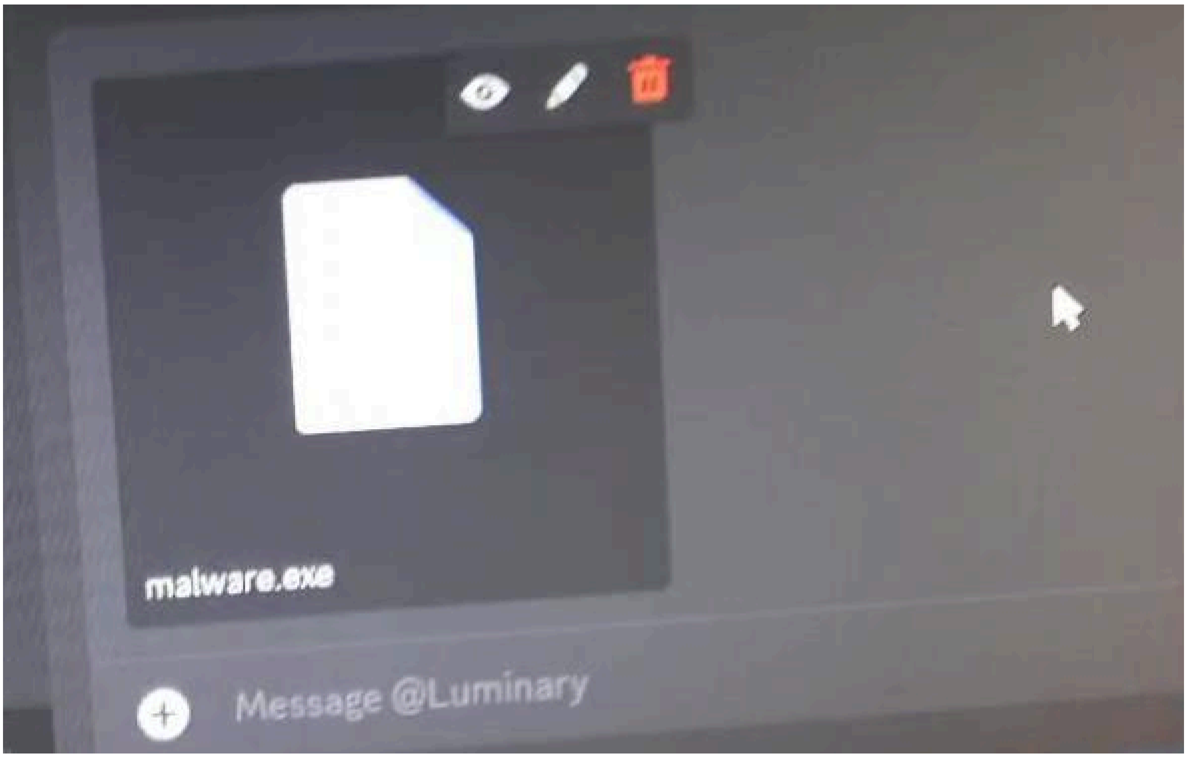
By Prv | mail | github | bugcrowd |

Name: Discord Windows Application - Executable Upload .com Bypass

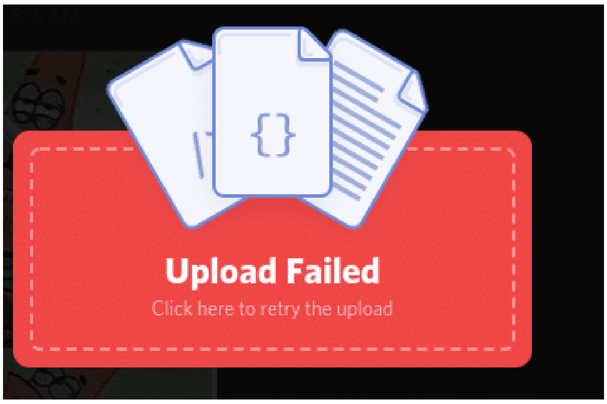
Vulnerability type: (CWE-434) - via Double File Extension Upload

Severity: **Medium⇒High**

When attempting to upload .exe files to another user's direct message chat was blocked by the discord application by doing so, this is done as standard to prevent users from distributing or potentially infecting other users with malicious software on the platform.



Upon further testing of this, realised that the application would not block or recognise files based of behaviours or contents- but rather only off file **extension type** and **file size**:

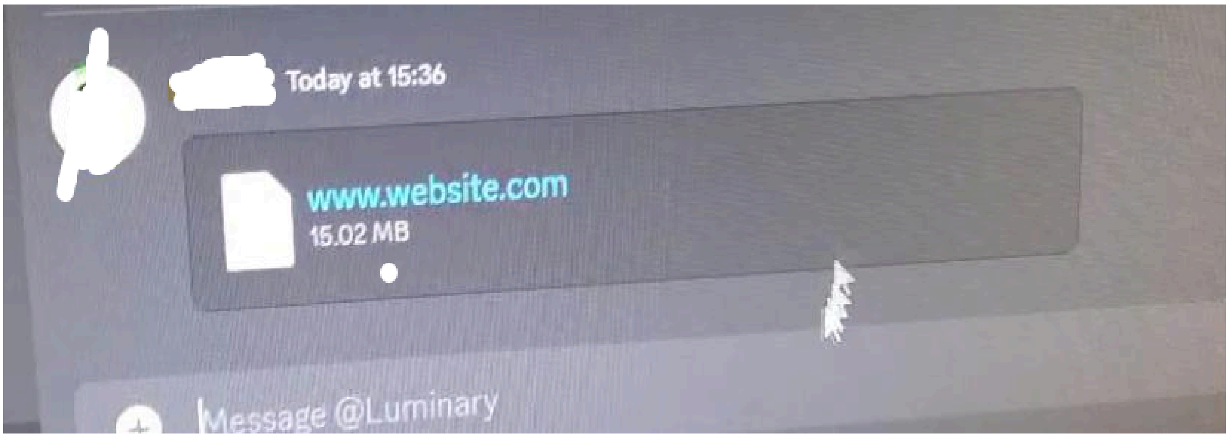


Due to this, was able to exploit this mechanism in the application by using a double file extension, using an executable type still perceived by the target system as executable and with compressed

contents, meaning the file was not traditionally flagged as potentially malicious and aligned with file size restrictions.

By doing this, I used (**.exe.com**) as my extension and compressed the size by obfuscating the code inside my program before compiling it, allowing me to upload and distribute malicious software:

This could also be done by tricking the application into thinking the uploaded executable was a hyperlink such as by renaming the file (**www.website.com)** This could also be used as a potential social engineering vector:



[redacted] Today at 15:36

www.website.com
15.02 MB

Resolution:

The issue was fully documented and reported, discord was made aware of this issue on the **2023/05/02** and was patched in the new discord update shortly after.

This document is a disclosed vulnerability report by a practised security researcher, all vulnerabilities and issues mentioned in this report have been released under the permission of the owner and/or have been mitigated against and fixed before this report was written, if by any chance the contents of this report can be replicated this is due to another vulnerability or mere coincidence, please report any issues or regards: prv@anche.no