ID	QUALTRICS ID	Threats description	Assumptions		STRIDE type	Affected Components
1	STOLEN-AUTH-INFO	Spoofing a remote repo admin by stealing the authentication credentials via a social engineering attack.	1. The attacker carries out a successful social engineering attack (attackers communicate legitimately with others, manipulating and exploiting human qualities to achieve their attack) and gets authentication credentials; 2. The credentials are valid.		spoofing	The remote code repository
2	LEAKED-CONFIG-FILE	An attacker uses leaked (e.g. on Github) configuration file to interact with the remote repo, potentially jeopardize running code and submitting malicious code.	1. The attacker finds the leaked information; 2. The attacker can (remotely) interact with the remote repo.		Information disclosure	Victim's server
3	DOS-SERVER	An attacker submit malicious code can crash the server running the code, causing a Denial of Service (DoS).	1. The attacker submits malicious code that can cause Denial of Service (DoS) to remote repo; 2. The server has pulled and been running the code submitted by the attacker.		DoS	Victim's server
4	MALICIOUS-CODE-GITHUB	An attacker submit malicious code to the project on GitHub and get a shell of the server running the code.	1. The attacker can submit code to remote repo; 2. The server has pulled and been running the malicious code submitted by the attacker.		Elevation of privilege	Victim's server
5	ELEVATION-PRIVILEDGED-ACCESS	The attacker uses the malicious code to gain root access to the server.	1. The attacker can submit code to remote repo; 2. The server has pulled and been running the code submitted by the attacker; 3. Code run as root on the server.		Elevation of privilege	Victim's server
6	DOS-REMOTE-REPO	The attacker submits the same fake push request to other remote code repositories, causing a Denial of Service attack.	1. Permission management is properly implemented in the remote (GitHub) provided repository hosting service to differentiate user access to the code repository; 2. An attacker has the right to submit a bogus push request to a remote repository.		DoS	Other remote code repositories
7	DISCLOSE-THIRD-PARTY	Not only can the attacker use these third-party services, but the attacker can also push code to the remote code repository where the yml file is located.	1. An attacker can browse the project's yml file; 2. The developer has left the keys to the third-party services they need to use in the yml file that configures GitHub Actions.		Information disclosure	Third-party services The remote code repository
8	ELEVATION-PRIVILEDGED-REPO	The attacker can launch a push request to a repository on GitHub and can delete the repository.	The attacker has gained push access to the code repository on GitHub.		Elevation of privilege	The remote code repository
9	ELEVATION-PRIVILEDGED-CODE	An unauthenticated and non privileged attacker can still submit custom code into the remote repo to prepare the first step of another attack, e.g. turning off logging service or cause a Denial of Service.	The attacker can reach the remote repo (e.g. through internet).		Elevation of privilege, Tampering	The remote code repository
10	EXPLOIT-HTTP-PROTOCOL	If an attacker compromises a http protocol on GitHub, the attacker can steal other users' identities by using HTTP by running a man in the middle attack.	1. GitHub uses the HTTPS protocol; 2. The attacker has compromised the HTTP protocol on GitHub.		Spoofing	GitHub engine