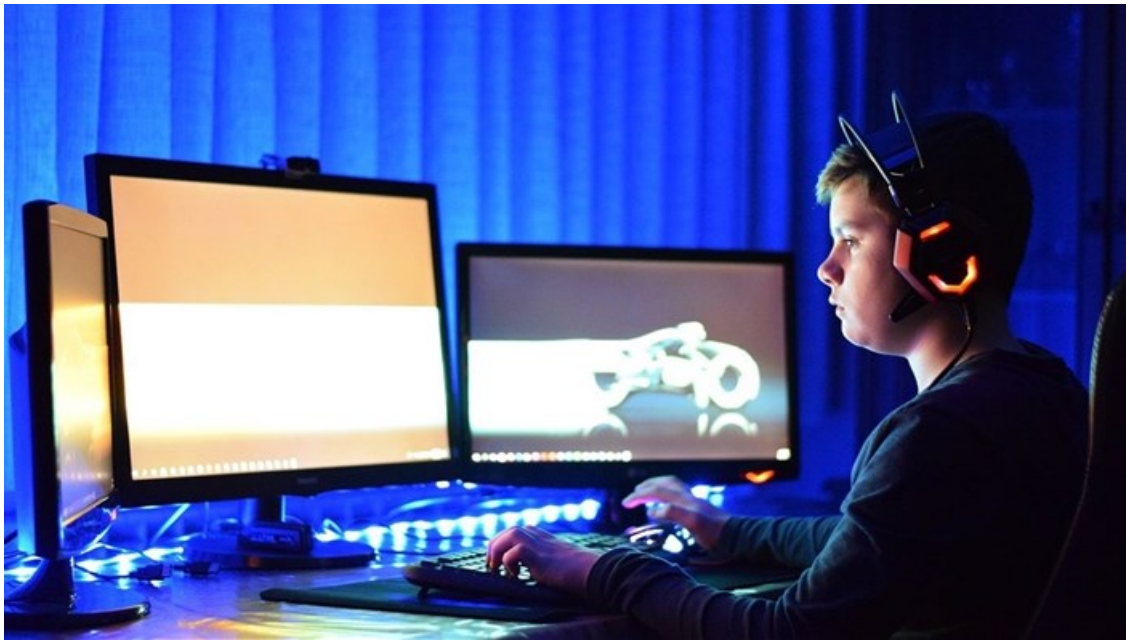
Check Point reveal vulnerabilities in online game

Researchers at Check Point Software Technologies, a provider of cyber security solutions globally, shared details of vulnerabilities that could have affected any player of the online battle game, Fortnite.



Source: pixabay.com

Fortnite has nearly 80 million players worldwide. The game is popular on all gaming platforms, including Android, iOS, PC via Microsoft Windows and consoles such as Xbox One and PlayStation 4. In addition to casual players, Fortnite is used by professional gamers who stream their sessions online and is popular with e-sports enthusiasts.

If exploited, the vulnerability would have given an attacker full access to a user's account and their personal information as well as enabling them to purchase virtual in-game currency using the victim's payment card details. The vulnerability would also have allowed for a massive invasion of privacy as an attacker could listen to in-game chatter as well as surrounding sounds and conversations within the victim's home or other location of play.

While Fortnite players had previously been targeted by scams that deceived them into logging into fake websites that promised to generate Fortnite's 'V-Buck' in-game currency, these new vulnerabilities could have been exploited without the player handing over any login details.

Vulnerabilities discovered in login process

Researchers outlined the process in which an attacker could have potentially gained access to a user's account through vulnerabilities discovered in Fortnite's user login process. Due to three vulnerability flaws found in Epic Games' web infrastructure, researchers were able to demonstrate the token-based authentication process used in conjunction with Single Sign-On (SSO) systems such as Facebook, Google and Xbox to steal the user's access credentials and take over their account.

To fall victim to this attack, a player needs only to click on a crafted phishing link coming from an Epic Games domain, to make everything seem transparent, though sent by the attacker. Once clicked, the user's Fortnite authentication token could be captured by the attacker without the user entering any login credentials.

According to Check Point's researchers, the potential vulnerability originated from flaws found in two of Epic Games' sub-domains that were susceptible to a malicious redirect, allowing users' legitimate authentication tokens to be intercepted by a hacker from the compromised sub-domain.

"Fortnite is one of the most popular games played mainly by kids. These flaws provided the ability for a massive invasion of privacy," said Oded Vanunu, head of products vulnerability research for Check Point.

"Together with the vulnerabilities we recently found in the platforms used by drone manufacturer DJI, show how susceptible cloud applications are to attacks and breaches. These platforms are being increasingly targeted by hackers because of the huge amounts of sensitive customer data they hold. Enforcing two-factor authentication could mitigate this account takeover vulnerability."

Users to remain vigilant

Check Point has notified Epic Games of the vulnerability which has now been fixed. Check Point and Epic Games advise all users to remain vigilant whenever exchanging information digitally and to practice safe cyber habits when engaging with others online. Users should also question the legitimacy of links to information seen on user forums and websites.

Organisations must perform thorough and regular hygiene checks on their IT infrastructure they have not left outdated and unused sites or access points online. In addition, it is good practice to review any outdated website or sub-domains that may still be online though not in use.

In order to minimise the threat of falling victim to an attack that exploits vulnerabilities like this, users should enable two-factor authentication, ensuring that when logging into their account from a new device, the player would need to enter a security code sent to the account holder's email addresses. It is also important that parents make their children aware of the threat of online fraud and warn them that cyber criminals will do anything to gain access to personal and financial details which may be held as part of a gamer's online account.

A full technical analysis of this vulnerability is available from the Check Point Research blog.

For more, visit: https://www.bizcommunity.com