Unity discloses a years-old security exploit and urges developers to update their games

Unity is urging developers to take “immediate action” after it disclosed a major security vulnerability affecting games built using versions of its popular development tool dating back to 2017. While there is “no evidence of any exploitation of the vulnerability, nor has there been any impact on users or customers,” Unity already has fixes available to developers, according to a post from Larry Hryb, aka “Major Nelson.”

Specifically, developers need to take action if “you have developed and released a game or application using Unity 2017.1 or later for Windows, Android, or macOS,” Hryb says. Unity’s “platform partners” have also “taken further steps to secure their platforms and protect end users.”

Valve already released a new version of Steam that adds mitigations for the exploit, and “for Windows, Microsoft Defender has been updated and will detect and block the vulnerability,” Hryb says. Google and Meta have taken steps as well, according to Hyrb. There are “no findings to suggest” that the vulnerability can be exploited on iOS, visionOS, tvOS, Xbox, Nintendo Switch, PlayStation, UWP, Quest, and WebGL.

Numerous developers have taken actions in response to the disclosure. Obsidian removed some of its games and products from digital storefronts, including *Grounded 2 Founders Edition*, *Avowed Premium Edition*, *Pillars of Eternity: Hero*

Edition, *Pillars of Eternity II: Deadfire*, and *Pentiment*, until it can "implement the necessary updates to address the issue." *Marvel Snap*, *No Rest for the Wicked*, *Ingress*, and *Fate/Grand Order* have all received updates as well. And Atlus says *Persona 5: The Phantom X* will get an update.

According to the Common Vulnerabilities and Exposures (CVE) record about the exploit, "if an application was built with a version of Unity Editor that had the vulnerable Unity Runtime code, then an adversary may be able to execute code on, and exfiltrate confidential information from, the machine on which that application is running."

***Update, October 3rd**: Added details about Obsidian removing games from storefronts and about games that have gotten updates.*

https://www.theverge.com/news/791609/unity-security-exploit-developers-update-games