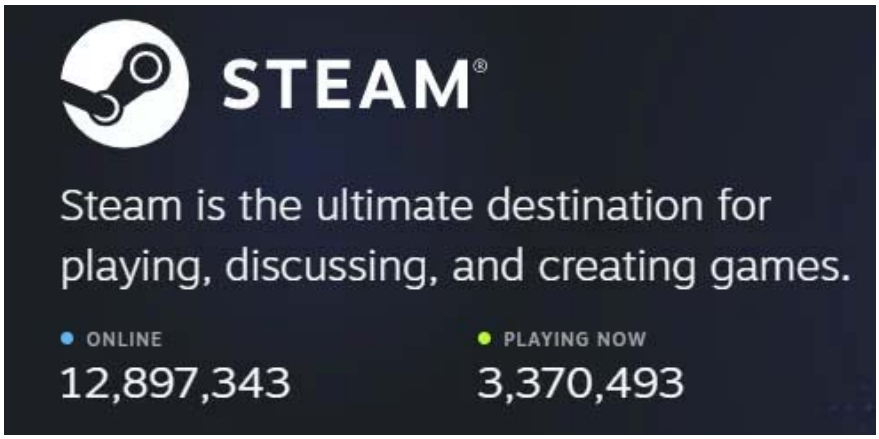
Discovering a new zero-day vulnerability in Steam, more than 100 million users may be affected

Steam currently contains a serious zero-day privilege escalation vulnerability.

Steam, one of the most widely reported online distribution platforms, digital copyright management, multi-player video games, and social communication services on the world's largest internet platform, contains one A serious zero-day privilege escalation vulnerability, which could allow an attacker to hijack many important system privileges, which are only used to run the program as an administrator.

If you do not know yet, Privilege escalation vulnerabilities are system errors that allow crooks to hold in their hands but limited rights to launch an executable file with advanced privileges or administrative rights. . According to statistics, Steam currently owns more than 100 million registered users and millions of online users on the platform at the same time, so this is a risk that is assessed at a very serious level, can create things. The case for an attacker to spread malware, thereby conducting many unauthorized activities can cause great damage to users if not patched in time.

1. Twitter appears 'error' that causes user information to be approached by third-party advertising providers



The vulnerability can affect millions of Steam users worldwide

Privileged breach vulnerability

Zero-day vulnerability on Steam was discovered by two security researchers not long ago and secretly reported back to Valve as part of a ransom-finding program. However, Valve's actions make many people disappointed that this vulnerability is "not applicable". The famous game developer chose to dismiss the findings of two security experts and decided to refuse to give error bonuses, as well as never give any indication that they would

mind or make any any measure to patch. The consequence is that this dangerous zero-day vulnerability has been made public, and now Valve is the one who has to find a way to respond.

1. Secure desktop application - weaknesses are often overlooked

Privilege escalation is one of the most dangerous security vulnerabilities

In a report published on August 8, veteran security researcher Felix analyzed a Windows service linked to Steam called "Steam Client Service" and pointed out the real possibility. Execute its system privileges (SYSTEM) on Windows platform. The security expert also found that the "Steam Client Service can be launched and stopped by the 'User' group.

However, the registry key for this service is not writable by the "User" group, so it will not be modified to launch another executable file, and escalate its privileges to administrators.

Another finding is also worth noting, that when this service is launched or stopped, it grants full access to the **subkeys** under the **HKLMSoftwareWow6432NodeValveSteamApps Registry key** .

The researcher then tried to configure a symbolic link from one of these subkeys to another that he did not own enough access to, and found that modifying the key was entirely possible.

With all the information collected, Felix realized that any Registry key could be modified by creating a symbolic link to it from a subkey in **HKLMSoftwareWow6432NodeValveSteamApps.**

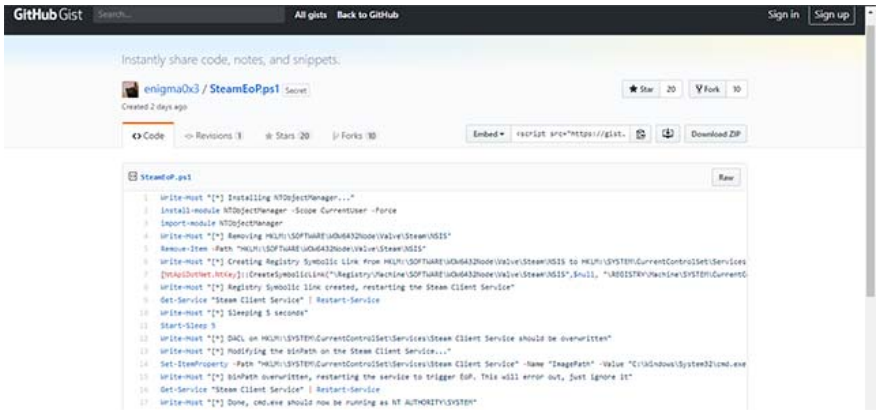
Thus, this may allow a service to run with modified system privileges, thereby launching another program with more important elevation rights.

1. British Airways has a systematic, delaying 'error' at many airports in the UK, customers dumping stones on Twitter

More findings from other researchers

After Felix revealed details of the vulnerability as mentioned above, another security researcher named Matt Nelson - who once resonated in the global security community after discovering a series of the privileged escalation vulnerability under the alias enigma0x3 last year - also created code-proof-concep (PoC) code on how to abuse the Steam vulnerability and publicly share it on GitHub.

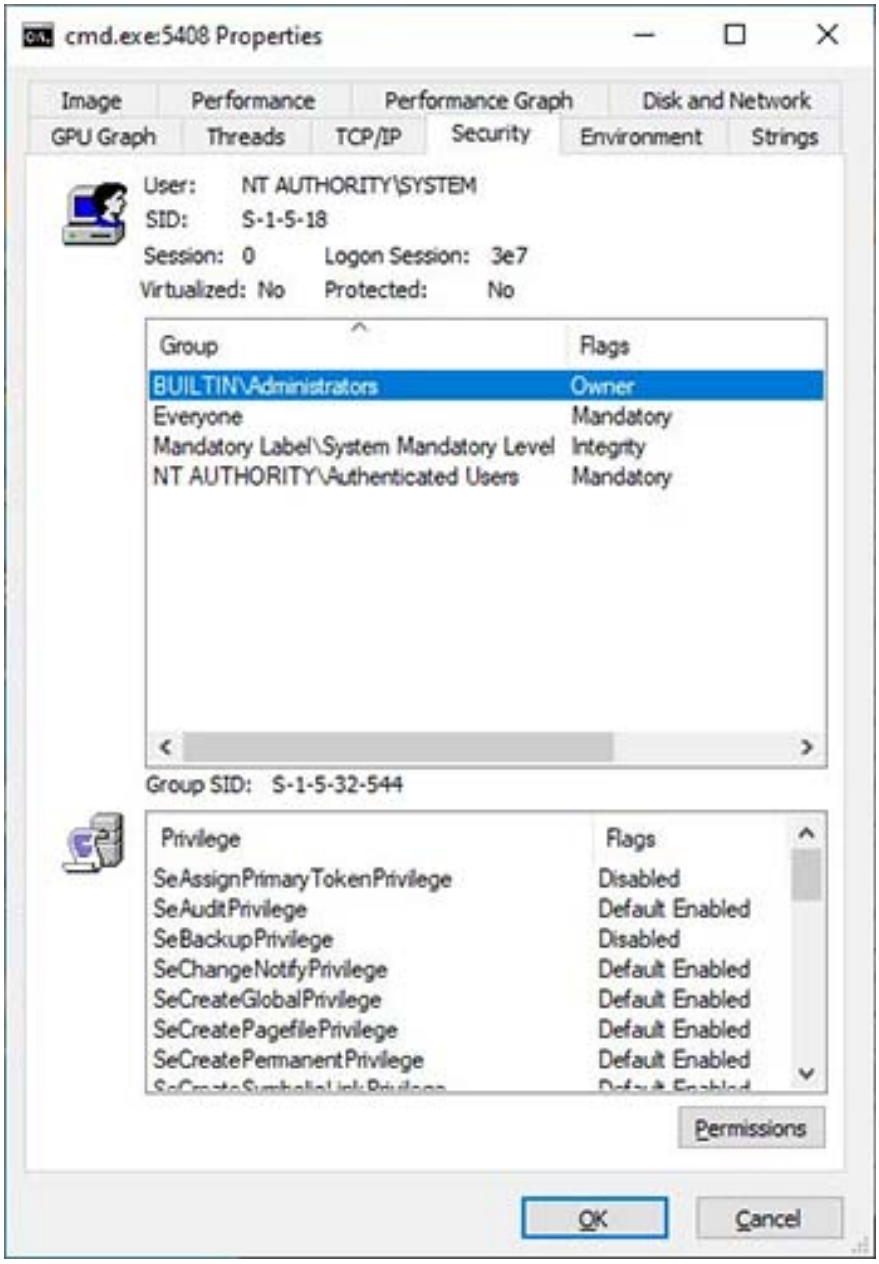
1. Honda's database leaked, revealing many "deadly" weaknesses in the intranet system



PoC code on how to abuse the vulnerability shared publicly by Matt Nelson on GitHub

Matt Nelson's PoC creates a symbolic link in the **HKLM: SYSTEMCurrentControlSetServicesSteam Client Service** so that the executable file can be changed automatically when the Steam Client Service is restarted.

This can be done by launching a Windows command prompt with Administrative privileges in the background, as shown in the illustration below.



Launch a Windows command prompt with administrative privileges in the background

Nelson said he also announced the issue with Valve but did not receive a reply.

Not only Matt Nelson, many major technology newspapers have also contacted Valve to find answers about why the vulnerability has not been fixed, but until now, this game developer remain silent.

As many experts have identified, this is a dangerous flaw and it needs to be patched as soon as possible. Valve's silence left many big question marks.

We will update the article as soon as we have the latest information!

1. ProFTPD remote code execution vulnerability affects more than 1 million servers worldwide

You finished reading the article "**Discovering a new zero-day vulnerability in Steam, more than 100 million users may be affected**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for

following us regularly.

© 2019 TipsMake.com