



Sign in

SigmaHQ / sigma Public

Notifications

Fork 2.2k

Star 8.3k

<> Code

Issues 11

Pull requests 33

Discussions

Actions

Wiki

Security

...

rule: susp svchost sub process #3946

New issue

Merged

Neo23x0 merged 3 commits into master from rule-devel on Jan 22, 2023

Conversation 4

Commits 3

Checks 0

Files changed



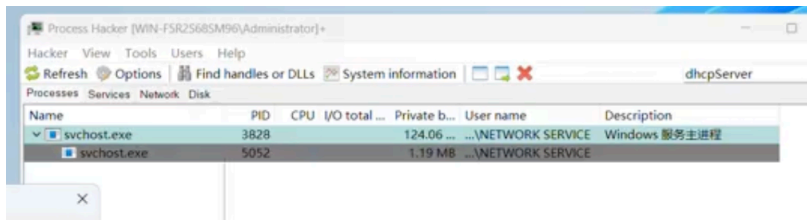
Neo23x0 commented on Jan 21, 2023

Collaborator



Trying to cover this unpatched RCE vulnerability

<https://twitter.com/YanZiShuang/status/1616777483646533632?s=20&t=TQT9tUuPbQJai4v6HtsOQw>



rule: susp svchost sub process

52a4985

Reviewers



nasbench



Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

Successfully merging this pull request may close these issues.

2 participants



nasbench commented on Jan 22, 2023

Member



There are actually 2 rules in the public repo that detect this behavior

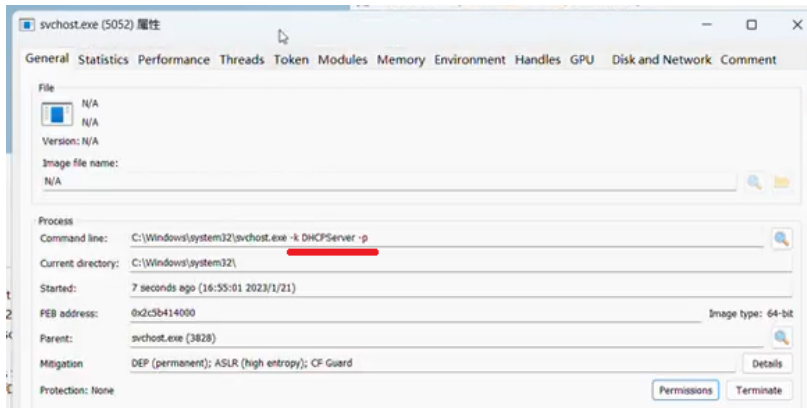
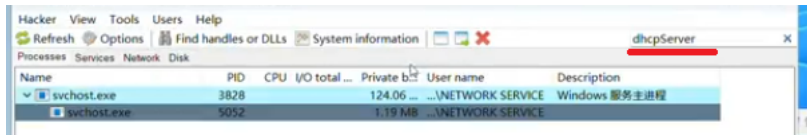
- [rules/windows/process_creation/proc_creation_win_susp_svchost.yml](#) -> Which looks for svchost process spawned from nonother than know processes such as a services.
- [rules/windows/process_creation/proc_creation_win_susp_svchost_no_cli.yml](#) -> Looks for svchost without CommandLine

And we also have a couple of private ones that check for svchost anomalies. So I think the behavior from the screenshot is already covered.



nasbench commented on Jan 22, 2023 • edited ▾ Member ...

Okay checking the video again I think we can pinpoint it further with the command line. Since he is filtering on the `dhcpserver` on the search bard that means that the command line is DHCPServer and we see that it spawns itself. So we can modify the rule accordingly since the vuln seems in that service.



nasbench added 2 commits [last year](#)

fix: add more detail a530e7a

fix: update filename f1c9112




nasbench approved these changes on Jan 22, 2023 [View reviewed changes](#)



Neo23x0 commented on Jan 22, 2023 [Collaborator](#) [Author](#) ...

Nice addition to make it more specific and good that you changed the title and description.



 **Neo23x0** merged commit **9739cb1** into **master**
on Jan 22, 2023



Neo23x0 commented
on Jan 22, 2023

Collaborator

Author



You should've added yourself to the authors

[Sign up for free](#) to join this conversation on GitHub. Already have an account? [Sign in to comment](#)

[Terms](#) [Privacy](#) [Security](#) [Status](#) [Docs](#) [Contact](#) [Manage cookies](#) [Do not share my personal information](#)



© 2024 GitHub, Inc.