

# Full Disclosure: Kms.nhp.gov.in Root Compromise

**Author:** Joakim Uddholm, tethik@blacknode.se

This document details how I was able to gain access to the root account and access the **kms.nhp.gov.in** host using the publicly exposed syncthing service.

All times are in UTC+02:00. While performing the attack I was using this IP: 176.125.235.113 (a commercial VPN).

## Background

[Syncthing](#) is a **continuous file synchronisation** program. It synchronises files between two or more computers in real time.

## Discovery

I initially discovered the host via shodan by searching for instances running syncthing. <https://www.shodan.io/host/117.239.179.28>

The screenshot displays the Shodan search results for the IP address 117.239.179.28. The interface is divided into several sections:

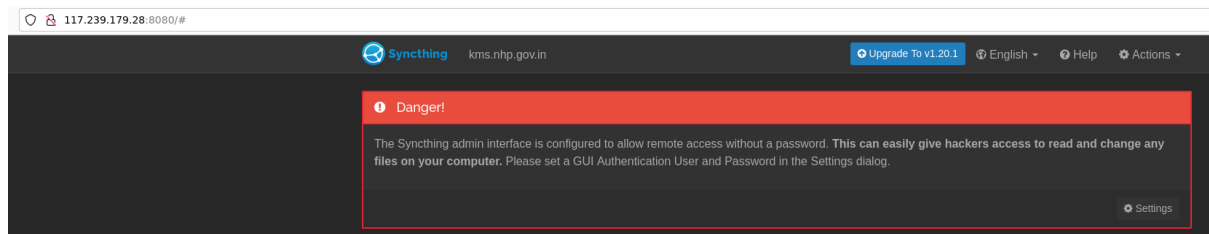
- General Information:** Lists hostnames (nhp.gov.in, kiosk.nhp.gov.in, static.ill.117.239.179.28/24.bun.in), domains (nhp.gov.in, 28), country (India), city (Mumbai), organization (NIB National Internet Backbone), ISP (National Internet Backbone), and ASN (AS9829).
- Web Technologies:** Lists technologies such as ANGULARJS, BOOTSTRAP, JQUERY, MOMENTJS, JWP PHP, and YUI.
- Vulnerabilities:** Lists several CVEs:
  - CVE-2018-15919:** Remotely observable behaviour in auth-gss2 in OpenSSH through 7.8 could be used by remote attackers to detect evidence of users on a target system when GSS2 is in use. NOTE: the discoverer states "We understand that the OpenSSH developers do not want to treat such a username enumeration for 'oracle' as a vulnerability".
  - CVE-2017-15906:** The process\_open function in sftp-server.c in OpenSSH before 7.6 does not properly prevent write operations in readonly mode, which allows attackers to create zero-length files.
  - CVE-2018-19935:** cmd/imap/imap.c in IMAP 5.x and 7.x before 7.3.0 allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via an empty string in the message argument to the imap\_mail function.
- Open Ports:** Shows a list of open ports, with OpenSSH 7.4 being the primary service. The OpenSSH 7.4 section includes the banner and key algorithms.

## Proof of Concept / Timeline

As an initial setup, syncthing was already running locally on the attacker's device.

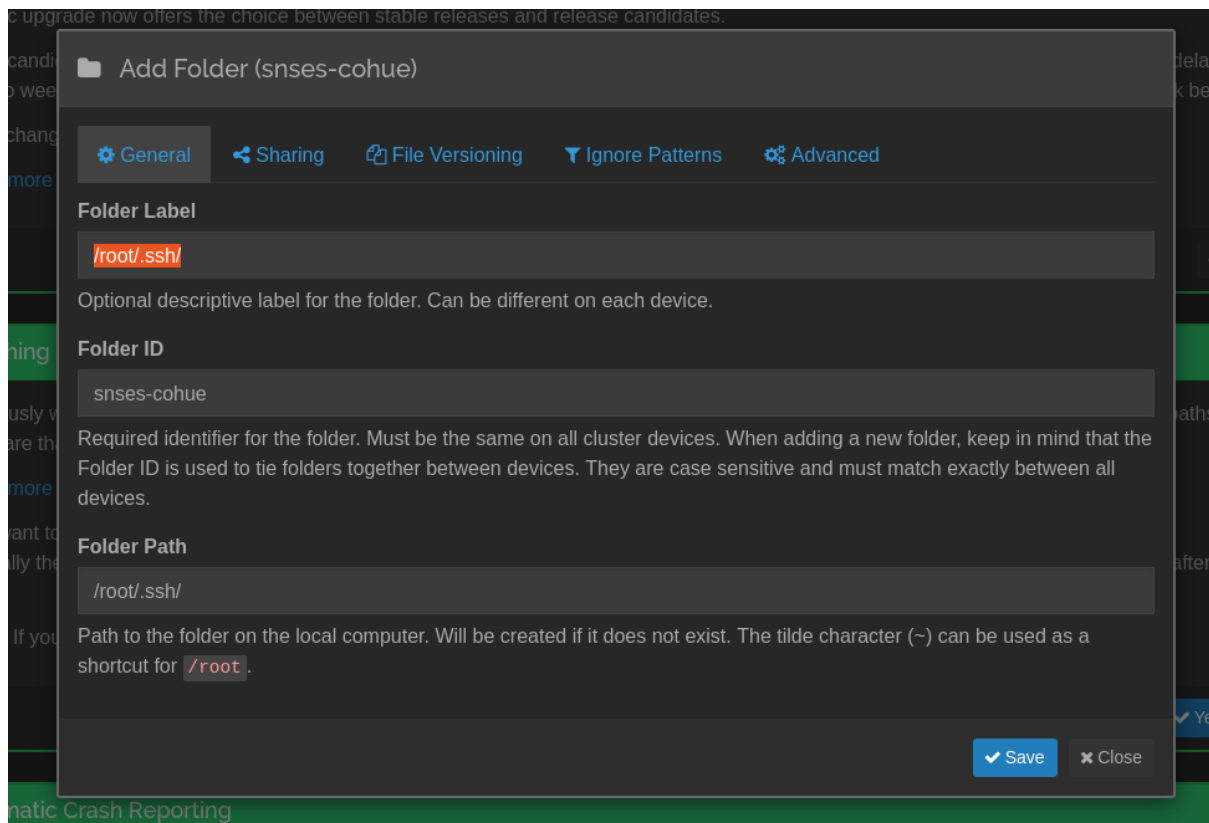
**2022-05-06 02:24:25** Accessing the indexed host on port 8080

(<http://117.239.179.28:8080/#>) shows the admin interface for the syncthing service.



Upon access, noted that there is no authentication set up.

**2022-05-06 02:25:00** Begin the attack by adding a new folder share for the `/root/.ssh/` folder.



**2022-05-06 02:34:58** Add the attacker device to attacker syncthing to allow syncthing to sync between the two hosts. The new `/root/.ssh` share is shared with the attacker device. The kms.nhp.gov.in device ID is also added on the attacker instance (UI in white).

### Add Device (OCHJUBB)

- General
- Sharing
- Advanced

#### Device ID

BRWPKXP-OCHJUBB-MXK3FQY-WHQ665Z-HPQZAXB-FAADYN7-37YTLZE-DKZKTQB

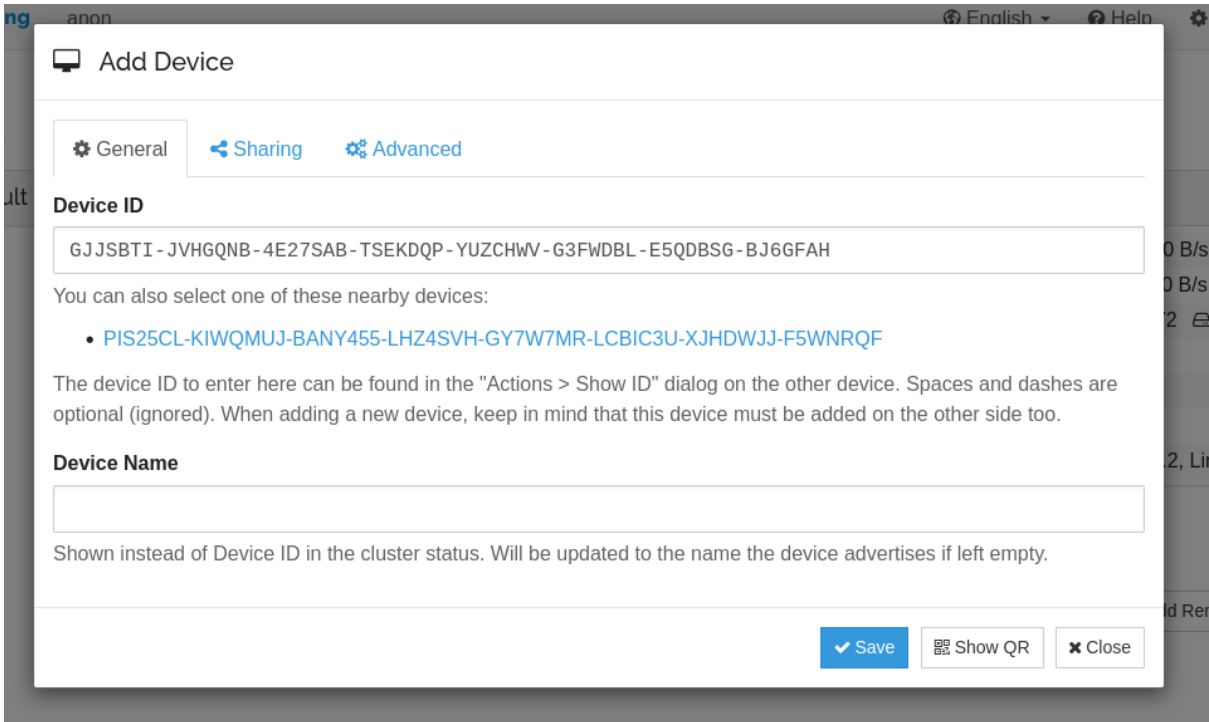
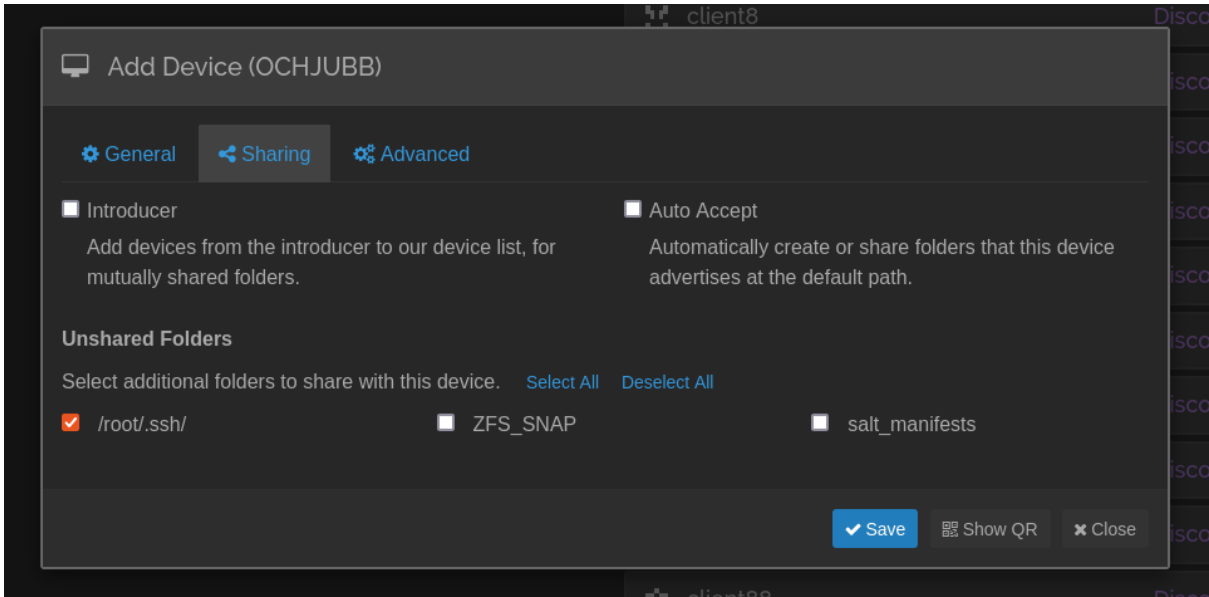
The device ID to enter here can be found in the "Actions > Show ID" dialog on the other device. Spaces and dashes are optional (ignored). When adding a new device, keep in mind that this device must be added on the other side too.

#### Device Name

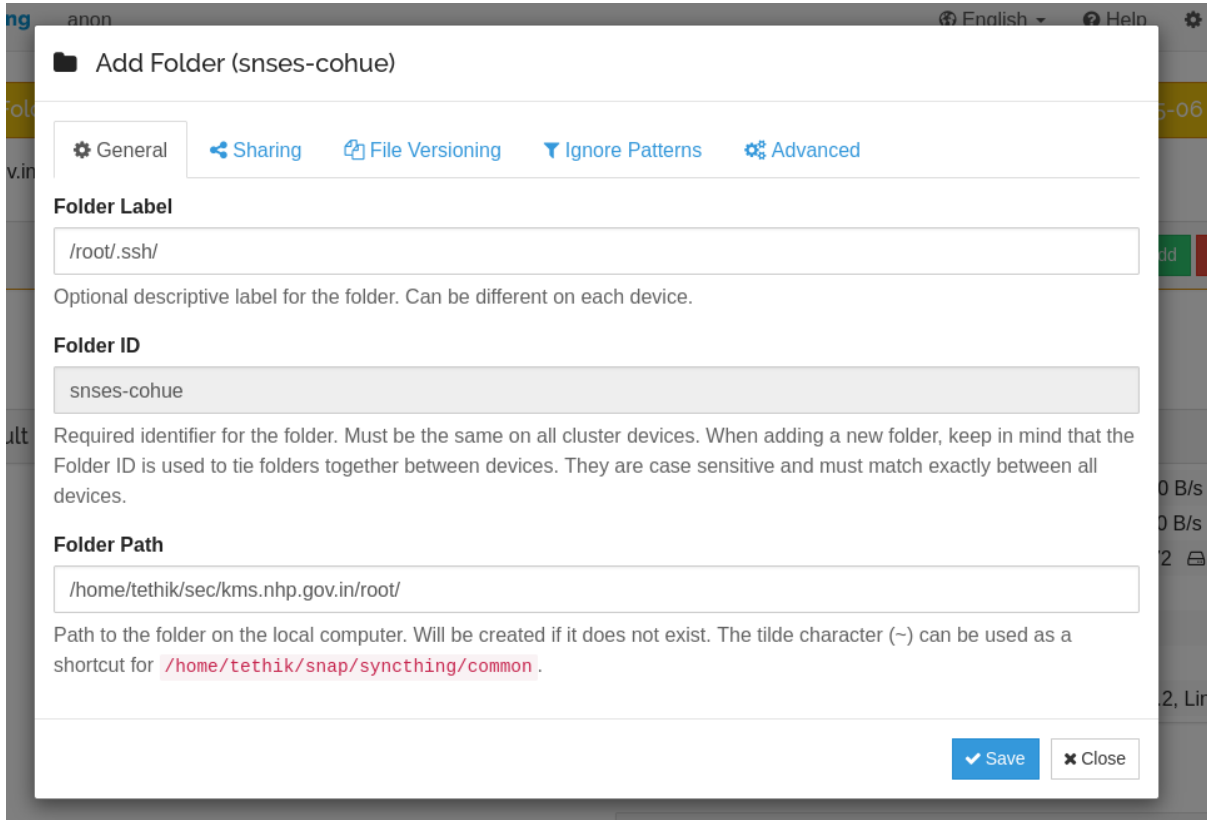
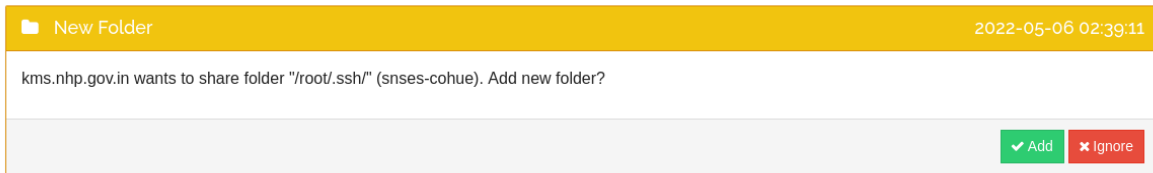
OCHJUBB

Shown instead of Device ID in the cluster status. Will be updated to the name the device advertises if left empty.

- Save
- Show QR
- Close




















**2022-05-06 02:39:51** After some time, the connection is synced between the devices. Attacker device is asked if it wants to accept the shared /root/.ssh folder.







2022-05-06 02:46:58 The /root/.ssh/ share finally syncs with the attacker host.

## Folders

 /root/.ssh/ Up to Date

 Folder ID	snses-cohue
 Folder Path	/home/tethik/sec/kms.nhp.gov.in/root/
 Global State	 4  0  ~7.95 KiB
 Local State	 4  0  ~7.95 KiB
 Rescans	 1h  Enabled
 Shared With	kms.nhp.gov.in
 Last Scan	2022-05-06 02:46:56
 Latest Change	Updated id_rsa

 Pause  Rescan  Edit

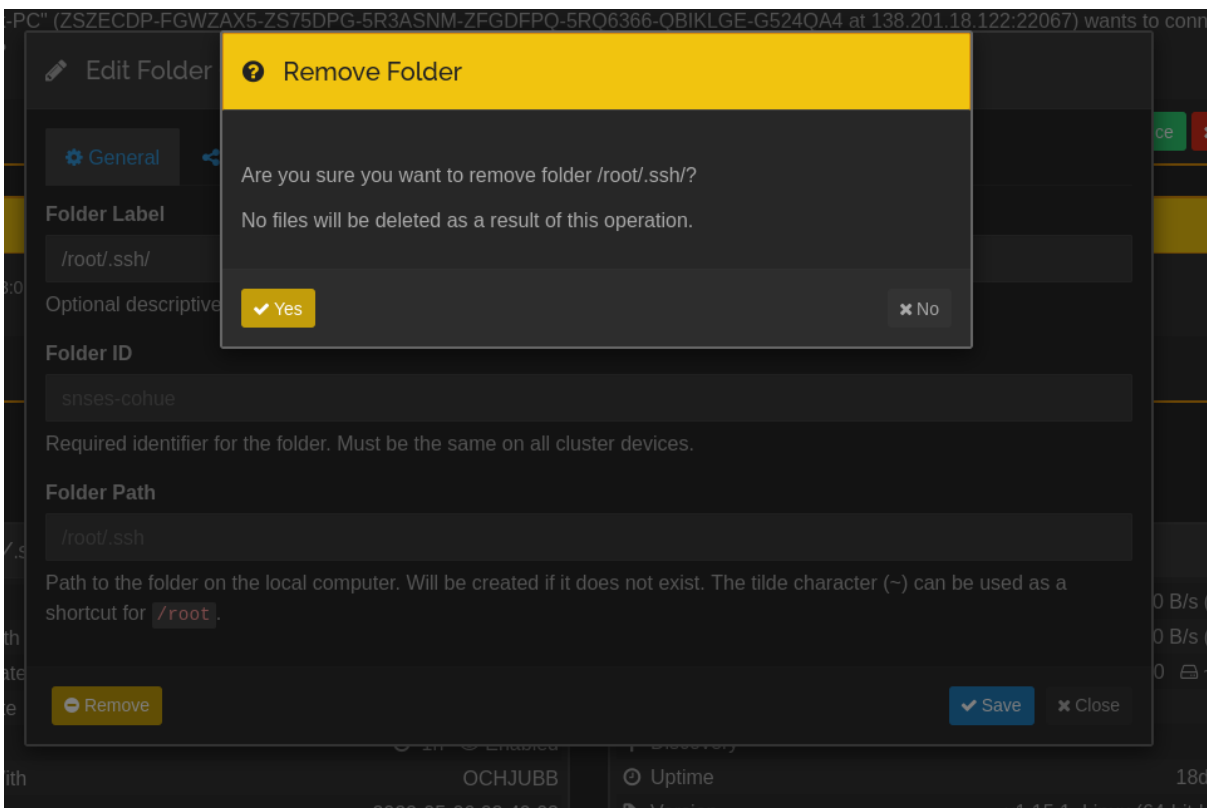
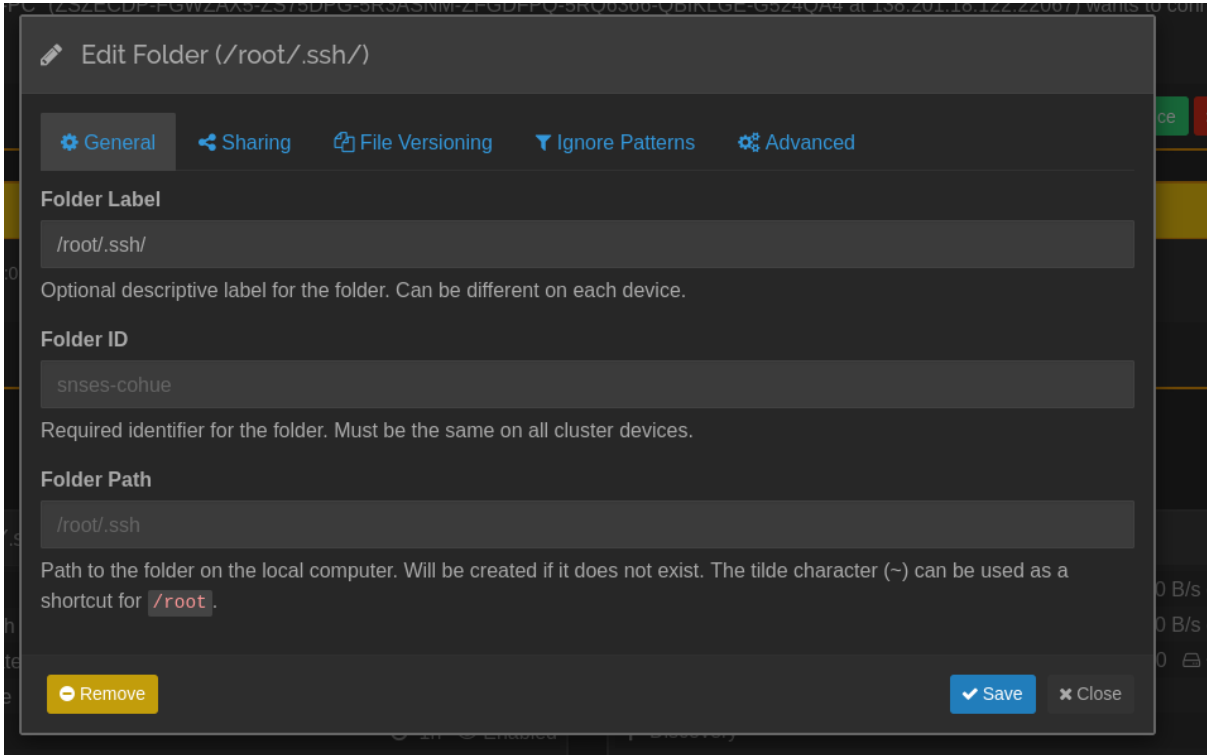
 Default Folder Paused

**2022-05-06 02:48:00** Attacker appends their ssh public key to the **authorized\_keys** file. After a second or two this file is synced to the kms.nhp.gov.in host. Attacker is then able to access the host via SSH. SSH Session Log will be attached separately.

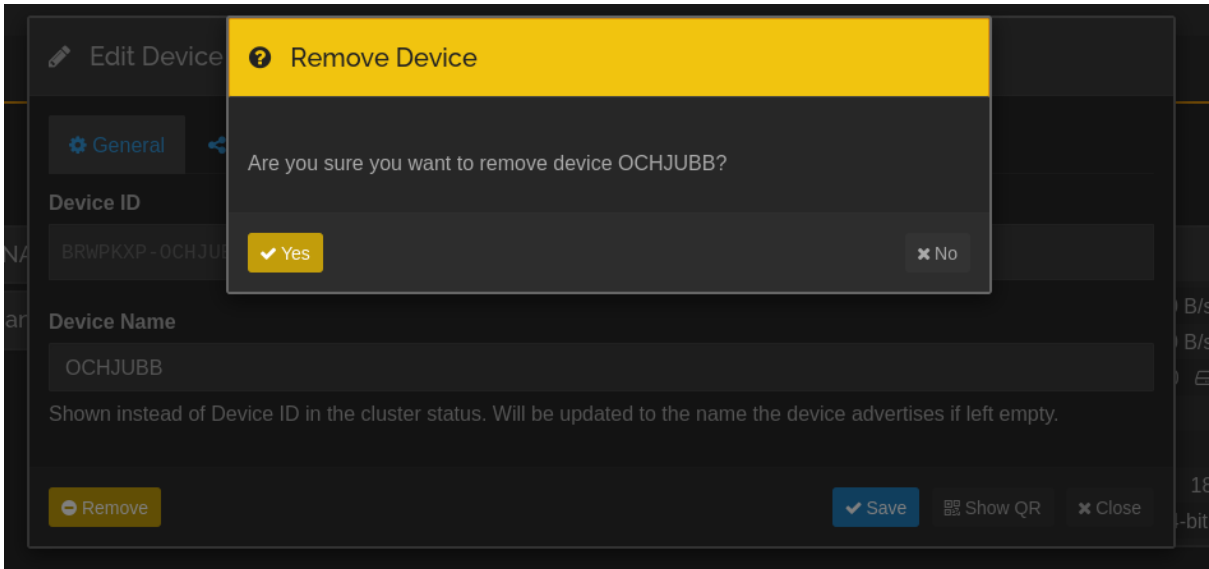
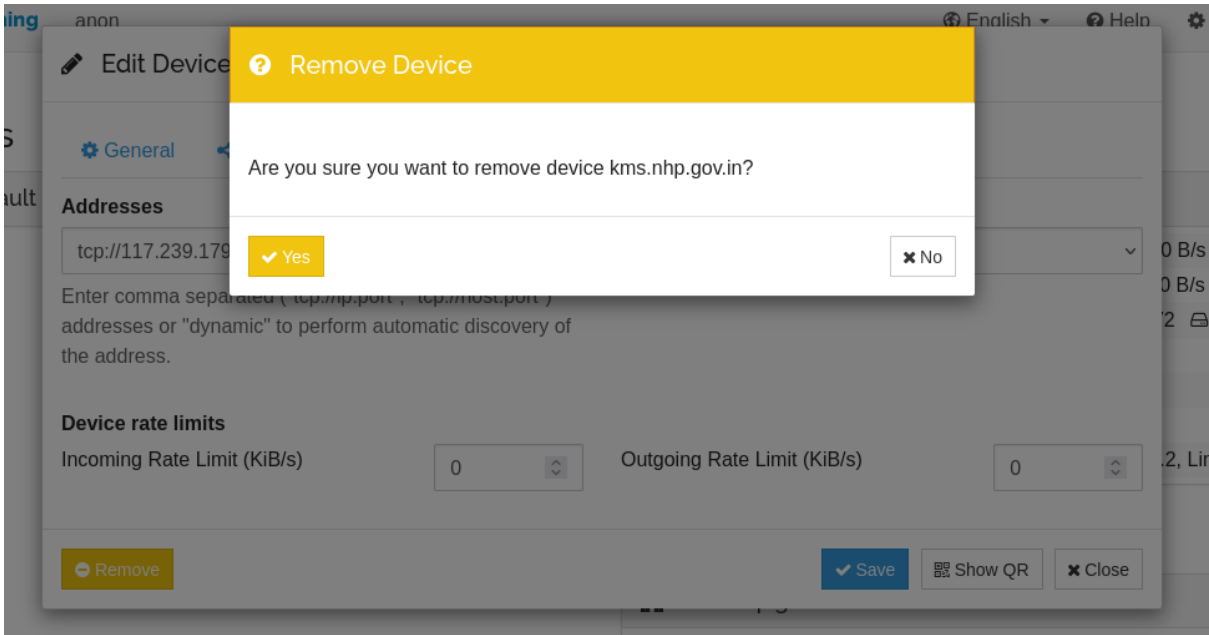
**authorized\_keys**

```
ssh-rsa
AAAAB3NzaC1yc2EAAAABJQAAAQEAEMvyUi5jXJnmI8cueOUSvOgSTpyGnSYp8to/Cx7Cy7nmK+nH1Qy70xcatertsVb5y
EtcbdLRD/YuchfQhXjdOz+twfep3HnH8OqEyLjH2VC9oEtlczmljLnkssWh091CQj//3khSHx9nOFEmuKtvs5tIH8pd9ojxp8BOG
2b0M9xGrG7Grz/uiSLG3jU3ahzRr24ixyh19GqC0A6fKp2feuh6tXqoS4GFioK8JaEeBUKpM/4D+FvGKrJwmZV015EK2SILpV
hpd5M5BqW9PM1mn2R49WkVaODCWxVVY/E2qJLB2M1dEo7bCMKe6qHZlzFdqfgzdMbzVP3AmY+dHhQ== 62mkv
office key
ssh-rsa
AAAAB3NzaC1yc2EAAAABJQAAAQEAmpFwu4R91zznFv7DnVr4atn7Mm8pa5gGRFm83NJMYcGSODefunJo/ONCNOPGn
ANSN8RcWYYarrLvm2/xqh7G/3YJdQazuNnYixAEhDdaiAA8wl+aIn2JHKMJ0QWvrNnh7uV0rRjr9cQ/wuyBnaYHKFx2l0g69
+42DOUiriBOA9b/BhckaOUWgeJxY9ogh5XW9i3swbSf0C685CDxaM27x/iKb64NdSn/qkcTatR48yGQ4VcrNhvZX1p9b40C3rl
qxsqP7/MsLjg3EETPaGcOSZ2mrCS0JcLWkCqQtLD2aCCFL/oszibNA0R+nDpplOpLN/RyLUwTpWzX1Dkt5rguRsw==
62mkv home rev2
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAQAC/URvqLVxxTdkCKzBmWA7JebB4g1OgmbNgX5vGnJ3pVqAXm6YLv7RHhDQ
RSapKUE4BcV5HVf072FFE0dT13szeP1H58sDRYUvru6i4NotrxHMWQxK7Kbtv5jrsyBghwXaVKTSl/YLb4X7koq/AVLXAzo
NkXgFVDRPTAM/vnr+pl3IOUArT13sRn/YTNmyEZ8Nrcwy61moJqiE0R26DWChv6aPOsFgMYhgwp7EvE1RkoJuzYi3MaCF
oi2URlesEAcl/JA4z9DyPuJ55N16U7VxONWjxgo87WiVRJbcnCpRBAG0pEZ95BtT8Z3CVpHJBttNG4PN1qo6c7OB6E1/5bn
R meny@meny-X555LD
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAQGBgQCChPtCmKqY63azNK4PLCIIl4yITuETfDNyzaZprulCtUiq4AJs4dBNTM/u/t
h+yL8PQAI1HJZMytrK6AEjXXLrjwcMX8nTdN9Cf4e77Keu5iizeeJojES+gh4tMbRO4px5Cx/ym4C2rJ9le6f2DPGIU3kfy
WeJoaKXM5T0sruezzehPI1VQ6icm1pHHdTf9ZU9Hv5qJU5xOxn+A8jWP668YF5DQ8Tq5qJbP4FD3Do2YlLHy/gxeV6
9dIM6XWFco3M0m/5MdckRz/KsCO5jh3VOF2ZyKsD/OKfJvCCw0HI7vTdc1B4khRQoIVYyBxluj8X4vxYK0Gj9C01HvEI
Fr9uo7Yof9G0tP1A+KxRHY+epKouEH8ep5jqOzQ92m4B9I728nHVheyIZVmX2rKG5s/yytJXkLI4vxv+ptZ+0A8HTbal37
B3FNd3O+KHSQhWdOkEr+/ZkHSnKcDMS/fjYiipcFd32zExmRtSCoulRdlIpOApxpd405LKZ/6WGPgDmk=
throwaway-key
```

2022-05-06 02:53:59 With the SSH access established, Folder share is deleted and device connection is removed.







2022-05-06 03:26:00 Initial reach out to CERT India.