Found 37 security holes in VNC on Linux, Windows

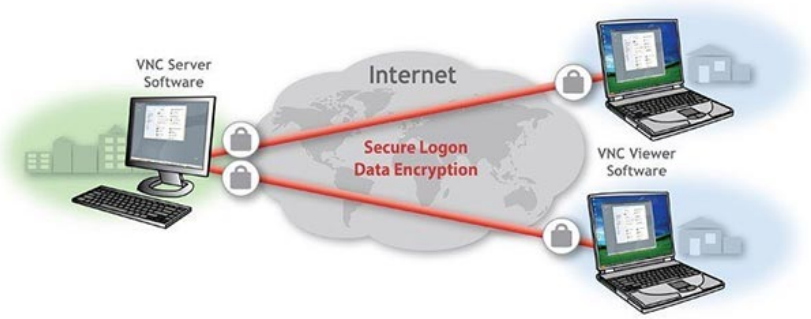
The researchers found a total of 37 security holes affecting four open source Virtual Network Computing (VNC) deployment solutions.

The researchers found a total of 37 security holes affecting four open source Virtual Network Computing (VNC) deployment solutions. Many of these have existed for more than 20 years, that is, from the late 20th century.

Specifically, the vulnerabilities were found in four VNC implementation solutions: LibVNC, TightVNC 1.X, TurboVNC and UltraVNC, by emergency security research team ICS CERT of Kaspersky. RealVNC - one of the extremely popular VNC solutions but not analyzed by unacceptable reverse engineering.

These VNC systems can be used on many famous operating systems, including but not limited to Windows, Linux, macOS, iOS and Android.

The deployment of VNC consists of two parts, the client and the server, allowing users to remotely access the system running the VNC server with the help of the VNC client using the RFB protocol to transmit "images." screen, data move mouse and press the "key.



More than 600,000 VNC servers are likely to be leaked

Kaspersky Lab's ICS CERT team found that more than 600,000 VNC servers can be accessed remotely via the Internet based on information collected by the Shodan search engine for Internet-connected devices - this estimate Excludes VNC servers running on local area networks.

The VNC security flaws that the team found were all due to inaccurate memory usage, with exploit attacks resulting in denial of service, glitches, as well as unauthorized access to people's information. use and execute malicious code on the target device. Many of these flaws have not been detected and fixed, even though they have existed for many years.

The full list of VNC vulnerabilities detected by the Kaspersky team is listed as follows:

LibVNC

1. CVE-2018-6307
2. CVE-2018-15126
3. CVE-2018-15127
4. CVE-2018-20019
5. CVE-2018-20020
6. CVE-2018-20021
7. CVE-2018-20022
8. CVE-2018-20023
9. CVE-2018-20024
10. CVE-2019-15681

TightVNC 1.X

1. CVE-2019-8287
2. CVE-2019-15678
3. CVE-2019-15679
4. CVE-2019-15680

TurboVNC

1. CVE-2019-15683

UltraVNC

1. CVE-2018-15361
2. CVE-2019-8258
3. CVE-2019-8259
4. CVE-2019-8260
5. CVE-2019-8261
6. CVE-2019-8262
7. CVE-2019-8263
8. CVE-2019-8264
9. CVE-2019-8265
10. CVE-2019-8266
11. CVE-2019-8267
12. CVE-2019-8268
13. CVE-2019-8269
14. CVE-2019-8270
15. CVE-2019-8271
16. CVE-2019-8272
17. CVE-2019-8273
18. CVE-2019-8274
19. CVE-2019-8275
20. CVE-2019-8276
21. CVE-2019-8277

22. CVE-2019-8280

Kaspersky offers the following suggestions to prevent exploitation of these VNC security holes:

1. Check if the device can connect remotely and block the connection remotely if not necessary.
2. Inventory all remote access applications - not just VNC - and check to see if their versions are the latest. If you have doubts about the reliability of the application, please stop using. If you intend to continue deploying them, upgrade to the latest version.
3. Protect your VNC server with a strong password. This will make the attack much harder.
4. Do not connect to untrusted or untested VNC servers.