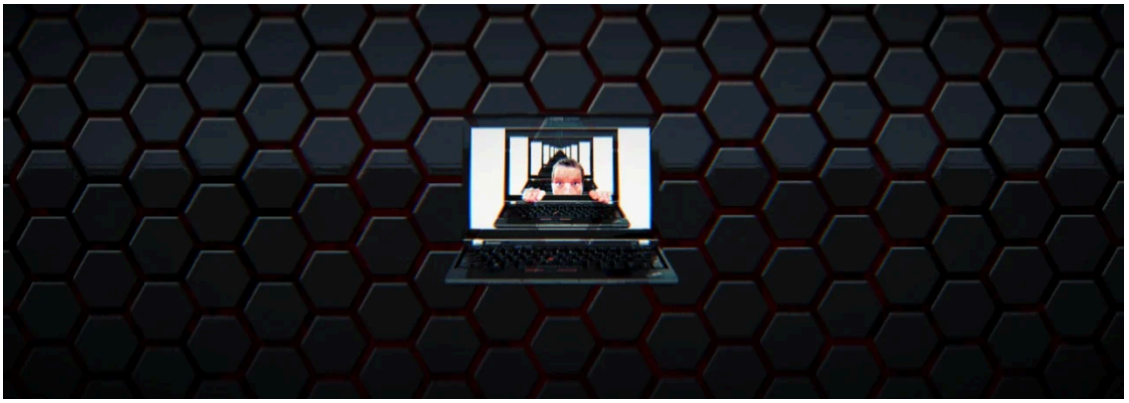
Dozens of VNC Vulnerabilities Found in Linux, Windows Solutions

By Sergiu Gatlan

Published: 2019-11-22 · Archived: 2026-04-05 12:40:58 UTC



Researchers found a total of 37 security vulnerabilities impacting four open-source Virtual Network Computing (VNC) implementations and present for the last 20 years, since 1999.

The flaws were found in LibVNC, TightVNC 1.X, TurboVNC, and UltraVNC VNC solutions examined by Kaspersky's Industrial Systems Emergency Response Team (ICS CERT) security researcher Pavel Cheremushkin — the highly popular RealVNC as not analyzed because it did not allow reverse engineering.

These VNC systems can be used on a wide range of operating systems including but not limited to Windows, Linux, macOS, iOS, and Android.


DIE LINKE.
0:00

A VNC implementation consists of two parts, a client and a server, allowing the users to remotely access a machine running the VNC server with the help of a VNC client using the RFB protocol to transmit "screen images, mouse movement and keypress events".

You can find more details about VNC implementations analyzed by Cheremushkin below:

> - LibVNC – an open-source cross-platform library for creating a custom application based on the RFB protocol. The server component of LibVNC is used, for example, in VirtualBox to provide access to the virtual machine via VNC.
> - UltraVNC – a popular open-source VNC implementation developed specifically for Windows. Recommended by many industrial automation companies for connecting to remote HMI interfaces over the RFB protocol.
> - TightVNC 1.X – one more popular implementation of the RFB protocol. Recommended by many industrial automation system vendors for connecting to HMI interfaces from *nix machines.
> - TurboVNC – an open-source VNC implementation. Uses the libjpeg-turbo library to compress JPEG images in order to accelerate image transfer.

Over 600,000 VNC servers potentially exposed

Based on this information, Kaspersky's ICS CERT researcher discovered over 600,000 VNC servers that can be accessed remotely over the Internet based on the info collected using the Shodan search engine for Internet-connected devices — this estimation doesn't cover the VNC servers running on local area networks.

The VNC security flaws Cheremushkin found are all caused by incorrect memory usage, with attacks exploiting them leading to denial of service states, malfunctions, as well as unauthorized access to the users' info and the option to run malicious code on a target's device.

"Although our colleagues' focus was on the use of VNC in industrial enterprises, the threats are relevant to any business that deploys this technology," the Kaspersky report adds.

While most of the VNC memory corruption vulnerabilities disclosed by the researchers to the development teams were fixed, in some cases they haven't been addressed to this day.

This is the case of TightVNC 1.X, whose developers said that they won't fix the found security issues since the software's first version is "no longer support the first version of their system [..]." They currently maintain the TightVNC 2.X commercial product.

Bugs found in VNC solutions

Cheremushkin found heap-based buffer overflows in the LibVNC library that could potentially allow attackers "to bypass ASLR and use overflow to achieve remote code execution on the client."

TightVNC came with a null pointer dereference leading to Denial of System (DoS) states, as well as two heap buffer overflows and a global buffer overflow that could lead to remote code execution. As already mentioned above, these security issues will not be fixed.

A stack buffer overflow vulnerability was discovered in the TurboVNC server the might lead to remote code execution, although it requires authorization on the server or control over the VNC client before the connection.

When it comes to UltraVNC, the researcher says that he was able to discover "an entire 'zoo' of vulnerabilities in UltraVNC – from trivial buffer overflows in strcpy and sprintf to more or less curious vulnerabilities that can rarely be encountered in real-world projects."

Out of all UltraVNC flaws he spotted, the buffer underflow one tracked as CVE-2018-15361 that can trigger a DoS in 100% of attacks but can also be used for remote code execution. The CVE-2019-8262 one is assigned to multiple heap buffer overflow vulnerabilities that can result in remote code execution.

The full list of discovered VNC vulnerabilities found by Kaspersky's Pavel Cheremushkin are listed in the table below:

VNC implementation	Vulnerabilities
LibVNC	• CVE-2018-6307 • CVE-2018-15126 • CVE-2018-15127 • CVE-2018-20019 • CVE-2018-20020 • CVE-2018-20021 • CVE-2018-20022 • CVE-2018-20023 • CVE-2018-20024 • CVE-2019-15681
TightVNC 1.X	• CVE-2019-8287 • CVE-2019-15678 • CVE-2019-15679 • CVE-2019-15680
TurboVNC	• CVE-2019-15683
UltraVNC	• CVE-2018-15361 • CVE-2019-8258 • CVE-2019-8259 • CVE-2019-8260 • CVE-2019-8261 • CVE-2019-8262 • CVE-2019-8263 • CVE-2019-8264 • CVE-2019-8265 • CVE-2019-8266 • CVE-2019-8267 • CVE-2019-8268 • CVE-2019-8269 • CVE-2019-8270 • CVE-2019-8271 • CVE-2019-8272 • CVE-2019-8273 • CVE-2019-8274 • CVE-2019-8275 • CVE-2019-8276 • CVE-2019-8277 • CVE-2019-8280

"On the positive side, password authentication is often required to exploit server-side vulnerabilities, and the server may not allow users to configure a password-free authentication method for security reasons. This is the case, for example, with UltraVNC," Cheremushkin concluded.

'As a safeguard against attacks, clients should not connect to unknown VNC servers and administrators should configure authentication on the server using a unique strong password."

Kaspersky provides the following recommendations to block attackers from exploiting these VNC security flaws:

• Check which devices can connect remotely, and block remote connections if not required.
• Inventory all remote access applications — not just VNC — and check that their versions are up-to-date. If you have doubts about their reliability, stop using them. If you intend to continue deploying them, be sure to upgrade to the latest version.
• Protect your VNC servers with a strong password. This will make attacking them far harder.
• Do not connect to untrusted or untested VNC servers.

Further information and more details on the VNC vulnerabilities discovered by Cheremushkin are available in the full VNC vulnerability research report available on the Kaspersky Lab ICS CERT website

---

Source: https://www.bleepingcomputer.com/news/security/dozens-of-vnc-vulnerabilities-found-in-linux-windows-solutions/