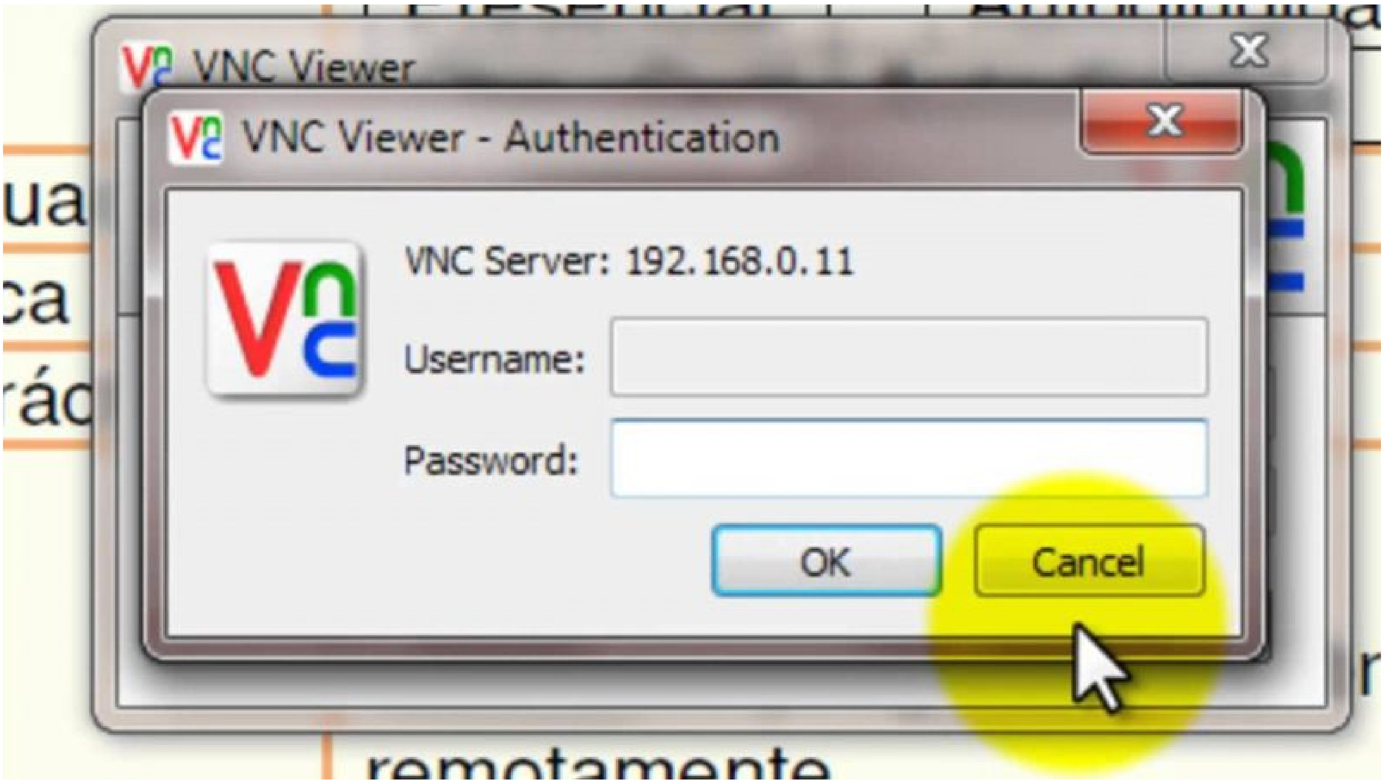
Critical Flaws in VNC Threaten Industrial Environments



VNC Server: 192.168.0.11

Author:
Tara Seals
November 22, 2019 / 2:50 pm

Share this article:

According to researchers at Kaspersky, they potentially affect 600,000 web-accessible servers in systems that use the code.

The research looked into four popular VNC-based systems, LibVNC, UltraVNC, TightVNC1.X and TurboVNC, which are actively used in automated industrial facilities to enable remote control of systems, according to the firm. Approximately 32 percent of industrial network computers having some form of remote administration tools, including VNC.

"The prevalence of such systems in general, and particularly ones that are vulnerable, is a significant issue for the industrial sector as potential damages can bring significant losses through disruption of complex production processes," Kaspersky researchers wrote in an analysis of the bugs for ICS CERT, released Friday.

Kasperksy found vulnerabilities not only in the client, but also on the server-side of the system; many of the latter however can only be exploited after password authentication. Across all 37 bugs, there are two main attack vectors, the firm said: "An attacker is on the same network with the VNC server and attacks it to gain the ability to execute code on the server with the server's privileges; [or] a user connects to an attacker's 'server' using a VNC client and the attacker exploits vulnerabilities in the client to attack the user and execute code on the user's machine."

A significant number of the problems detailed in the research were found and reported last year; however, each of the projects examined also had newly discovered bugs.

For instance, a newly found critical (9.8 out of 10 on the CVSS v.3 severity rating scale) database stack buffer overflow vulnerability in the TurboVNC server code could result in RCE. The issue (CVE-2019-15683) exists because the stack frame is not protected with a stack canary. However, to exploit the bug, authorization on the server is required.

"Some compilers perform…optimizations by removing stack canary checks from the functions that don't have explicitly allocated arrays," according to the research. "However, the compiler could make a mistake and fail to check for the presence of a buffer in some of the structures on the stack or in switch-case statements."

Also, a critical integer-overflow vulnerability (CVE-2018-15361) exists in UltraVNC client-side code. This is also critical, with a CVSS rating of 9.8 o

denial-of-service state. Researchers also "wouldn't r

sufficient memory, a large buffer will be allocated, w right parameters, a remote attacker would be able to write a null byte to the _NT_HEAP structure, which will be located directly before a huge chunk."

Meanwhile, the CVE-2019-8262 critical vulnerability (with a CVSS score of 9.8 out of 10) was identified in the handler of data encoded using the UltraVNC encoding function that could cause information disclosure.

"The uninitialized variable new_len is passed to the lzo1x_decompress function," according to the research. "At the time of calling the function, the variable should be equal to the length of the m_zlibbuf buffer…since the variable new_len was not initialized, it contained a large text section address value. This made it possible for a remote user to pass specially crafted data to the decompression function as inputs to ensure that the function, when writing to the m_zlibbuf buffer, would write the data beyond the buffer's boundary, resulting in heap overflow."

In TightVNC code version 1.3.10, there's a critical global buffer overflow (CVE-2019-8287) in HandleCoRREBBP macro function, also with a CVSS rating of 9.8 out of 10. This can also potentially result RCE, Kaspersky found.

Researchers also recently found a high-severity flaw in LibVNC (CVE-2019-15681), with a CVSS rating of 7.7 out of 10. It involves a memory leak exploitable via network connectivity in the VNC server code, which allows an attacker to read stack memory and can be abused for information disclosure. According to the advisory, combined with another vulnerability, it can be used to leak stack memory and bypass ASLR.

Worryingly, some of the bugs had been incorporated into the VNC code for years, meaning that projects built on it have "inherited" the issues.

"I was surprised to see the simplicity of discovered vulnerabilities, especially considering their significant lifetime," said Pavel Cheremushkin, Kaspersky ICS CERT vulnerability researcher, in a media statement. "This means that attackers could have noticed and taken advantage of the vulnerabilities a long time ago. Moreover, some classes of vulnerabilities are present in many open-source projects and remain there even after refactoring of the [main] codebase."

Kaspersky contacted the affected developers, and patches have been issued for supported products, it said. TightVNC for instance has discontinued the development of the TightVNC 1.X line and considers it end of life, so the bugs won't be patched.

Is MFA enough to protect modern enterprises in th

Write a comment

Share this article:

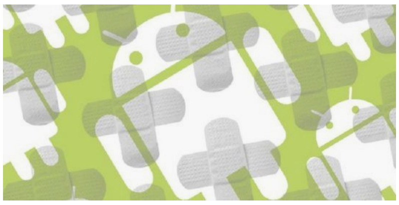
Critical Infrastructure Vulnerabilities

SUGGESTED ARTICLES

ThreatList: A Third of Biometric Systems Targeted by Malware in Q3

A successful attack could wreak havoc, given the potential for biometric forgery, and a lack of options in the event one's biometric profile is stolen.

December 3, 2019 1



Critical Android Flaw Leads to 'Permanent DoS'

The December security update stomped out critical denial-of-service (DoS) and remote-code-execution (RCE) vulnerabilities in the Android operating system.

December 3, 2019

Smart TVs: The Cyberthreat Lurking in Your Living Room, Feds Warn

TV takeover, privacy threats, botnet concerns and Wi-Fi network compromise are all big concerns when it comes to connected TVs.

December 2, 2019

DISCUSSION

Leave A Comment

Write a reply...

Your name

Your email

□ I'm not a robot

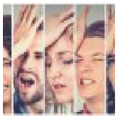
reCAPTCHA
Privacy - Terms

This site uses Akismet to reduce spam. Learn how your comment data is processed.

INFOSEC INSIDER

Managing the Human Security Factor in the Age of Ransomware

November 26, 2019 1



Three Areas to Consider, to Focus Your Cyber-Plan

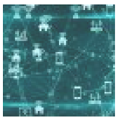
November 22, 2019

Website, Know Thyself: What Code Are You Serving?

November 14, 2019

Plugging the Data Leak in Manufacturing

November 12, 2019



Art Imitates Life: Lessons from the Final Season of Mr. Robot

November 8, 2019 2

Subscribe now

Subscribe now

threatpost The First Stop For Security News

Privacy Policy

Terms and Conditions

Advertise