Check Point Identifies Security Flaws In Apache Guacamole, The Widely Popular Remote Working Gateway Software

Published on 3 Jul 2020

Researchers at Check Point have identified security flaws in Apache Guacamole, one of the world’s most popular IT infrastructures for remote work. With over 10 million downloads, the free open-source software enables remote workers to access their company’s computer network from anywhere, by using only a web browser.

Apache Guacamole software

Apache Guacamole runs on many devices, including mobile phones and tablets, giving remote workers ‘constant, world-wide, unfettered access to computers’, according to the software’s creators.
Eyal Itkin, a Vulnerability Researcher at Check Point, demonstrated that a threat actor with access to a computer inside an organization can execute a Reverse RDP attack, an attack in which a remote PC infected with certain malware takes over a client that tries to connect to it.

**Reverse RDP attack**

Once in control of the gateway, an attacker could eavesdrop on all incoming sessions

In this case, the Reverse RDP attack would enable a threat actor to take control of the Apache Guacamole gateway that handles all of the remote sessions in a network. Once in control of the gateway, an attacker could eavesdrop on all incoming sessions, record all the login credentials used, and even control other sessions within the organization.

Check Point researchers say this foothold is equivalent to gaining full control over the entire organizational network. Check Point researchers classified their findings into two attack vectors:

- **Reverse Attack Scenario:** A compromised machine inside the corporate network leverages the incoming benign connection to attack the Apache gateway, aiming to take it over.

- **Malicious Worker Scenario:** A rogue employee uses a computer inside the network to leverage his hold on both ends of the connection and take control of the gateway.

**Data security in remote work operations**

Omri Herscovici, Vulnerability Research Team Leader at Check Point said, “While the global transition to remote work is a necessity, we cannot neglect the security implications of such remote connections, especially as we enter the post-coronavirus era. This research demonstrates how a quick change in the social landscape directly affects what attackers might focus their efforts on. In this case, it’s remote work.”
Omri adds, “The fact that more and more companies have externalised many internally-used services to the outside world opens a number of new potential attack vectors for threat actors. I strongly urge companies and organizations to keep their servers up-to-date to protect their remote workforces.”

Check Point Research responsibly disclosed its findings to The Apache Software Foundation (Apache), the maintainers of Guacamole, on March 31, 2020. On May 12, Apache issued 2 CVE-IDs to the 4 reported vulnerabilities, and Apache has released a patched version in June 2020.
The safeguarding of premises through the monitoring of entrance and exit points has traditionally been a very manual aspect of security. Hum...

In the past three two weeks, Check Point researchers have documented an average of 192,000 Coronavirus-related cyberattacks per week, markin...

Check Point has introduced CloudGuard Cloud Native Security, a fully-automated cloud platform that enables customers to seamlessly protect a...

The unprecedented global impact of COVID-19 has taken its toll on all of us, but as cases of the virus thankfully recede, employers are now...