McAfee software has a vulnerability that allows hackers to run code with system privileges on Windows

This vulnerability was patched shortly after McAfee Enterprise received a report from security researchers.

McAfee Enterprise (recently renamed Trellix) has patched a critical vulnerability in its McAfee Agent software for Windows. This vulnerability allows hackers to elevate privileges and run arbitrary code with system privileges on Windows.

McAfee Agent is a client-side component of McAfee ePolicy Orchestrator (McAfee ePO) that downloads and enforces endpoint policies and deploys anti-virus signatures, upgrades, patches, and new products on enterprise endpoints. Karma.

According to McAfee, this is a severe local privilege escalation (LPE) vulnerability and is tracked under the code CVE-2022-0166. This vulnerability was discovered by CERT/CC vulnerability analyst Will Dormann. The vulnerability was patched in the McAfee Agent 5.7.5 update released on January 18.

All versions of McAfee Agent older than 5.7.5 are vulnerable and allow unprivileged hackers to run code using the NT AUTHORITYSYSTEM privileged account, the highest level of privilege on a Windows system. NT AUTHORITYSYSTEM is commonly used by the operating system and its services.

"McAfee Agent is bundled with various McAfee products such as McAfee Endpoint Security, which includes an OpenSSL component that specifies an OPENSSLDIR variable as a subdirectory that can be controlled by users without Windows privileges," Dormann shared. shall.

"McAfee Agent contains a privileged service that uses this SSL component. Users who can place the specially crafted openssl.cnf file at an appropriate path can execute arbitrary code with system privileges. system".

After successfully exploiting the vulnerability, the hacker can continuously execute malicious software and potentially avoid detection during the attack. Hackers often use this form of LPE vulnerability in the later stages of attacks. After infiltrating the target's system, LPE is used to increase privileges to maintain the presence of malicious code, continuing to penetrate deeper into the system.

This isn't the first time security researchers have found vulnerabilities in McAfee's Windows security products.

For example, in September 2021, the company patched another privilege escalation vulnerability in McAfee Agent (CVE-2020-7315) discovered by Tenable security researcher Clement Notin. CVE-2020-7315 allows hackers to execute arbitrary code and disable antivirus.

Two years ago, McAfee patched a security vulnerability that affected all versions of anti-virus software for Windows (such as Total Protection, Anti-Virus Plus, and Internet Security) and allowed hackers to elevate privileges and execute code with system account.