



May 11, 2021

# PRIVILEGE ESCALATION VULNERABILITY IN NINJARMM AGENT MSI INSTALLER INTRODUCED BY EXEMSI MSI WRAPPER

powered by:

Cookie Information (<https://cookieinformation.com/>)

You control your data

We and our business partners use technologies, including cookies, to collect information about you for various purposes, including:

1. Functional
2. Statistical
3. Marketing

Martin Sohn Christensen (/tech-blog?author=6098d928cf0fa94ff1030fda)

By clicking 'Accept', you give your consent for all these purposes. You can also choose to specify the purposes you consent to by ticking the checkbox. During a customer engagement meeting, I discovered a local escalation of privilege vulnerability (CVE-2021-26273 (<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-26273>)) in the remote monitoring and management (RMM) tool: NinjaRMM Agent. The vulnerability allowed a non-administrative user to become an NT Authority\SYSTEM.

You can read more about how we use cookies and other technologies and how we collect and process personal data by clicking the link. [Read more about cookies](#)

Since the RMM tool was deployed on most of the customer's systems, the newfound vulnerability, in combination with lateral movements, made it easy to compromise any of the customer's most critical systems.

Post-discovery, I went on to talk with NinjaRMM who identified the vulnerability stemming from a tool in their software: EXEMSI MSI Wrapper which allows a software vendor to "wrap" an EXE-file in an MSI-file which allows easier deployment. The MSI Wrapper itself and systems with it installed are not vulnerable, but any MSI-files created with the tool could be (CVE is pending).

I have spent additional time identifying and contacting other software vendors using MSI Wrapper to ensure they are aware of this and mitigate the vulnerability in their newest deployments.

I also discovered an additional vulnerability (CVE-2021-26274 (<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-26274>)) in the NinjaRMM Agent, not nearly as interesting, but a vulnerability, nonetheless.

Both vulnerabilities of NinjaRMM Agent are described in this blogpost. The local privilege escalation vulnerability exploitation steps will vary depending on how the software vendor customizes the MSI-file and how the MSI-file is deployed.

## CVES REGISTERED

- NinjaRMM Agent
  - CVE: CVE-2021-26273 (<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-26273>)
  - CVE: CVE-2021-26274 (<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-26274>)
  - Update regarding the CVEs from Ninja (<https://www.ninjaone.com/blog/cve-2021-26273-cve-2021-26274/>)

## AFFECTED VERSIONS

- EXEMSI MSI Wrapper prior to version 10.0.50 and at least since version 6.0.91
- NinjaRMM Agents prior to version 5.0.4.0, since version 4.0.0