RCE via Actions and JSON Deserialization Vulnerability (CVE-2021-31474)

Security Advisory Summary

This vulnerability allows remote attackers to execute arbitrary code on affected installations of SolarWinds Network Performance Monitor 2020.2.1. Authentication is required to exploit this vulnerability. The specific flaw exists within the SolarWinds.Serialization library. The issue results from the lack of proper validation of user-supplied data, which can result in deserialization of untrusted data. An attacker can leverage this vulnerability to execute code in the context of SYSTEM. Was ZDI-CAN-12213.

Affected Products

- Orion Platform 2020.2.4 and earlier

Fixed Software Release

- Orion Platform 2020.2.5

Acknowledgments

- Chudy working with Trend Micro Zero Day Initiative