

Five Vulnerabilities SVR is Exploiting Right Now and How to Stop Them

UNDERSTAND THE THREAT

The Russian Foreign Intelligence Service, known as SVR, poses a significant risk to U.S. and allied government networks. In addition to having compromised SolarWinds Orion software updates recently, SVR cyber actors are exploiting at least five publicly known vulnerabilities to gain footholds into victim networks. Network defenders should take action to mitigate compromises and prevent future loss of sensitive information.

Publicly known vulnerabilities SVR is exploiting:

CVE-2018-13379

CVE-2019-9670

CVE-2019-11510

CVE-2019-19781

CVE-2020-4006

TAKE ACTION



Update systems and products as soon as possible after patches are released.



Reduce exposure of the local network by separating internet-facing services into a small, isolated network.



Assume a breach will happen; review accounts and leverage the latest eviction guidance available.



Enable robust logging of internet-facing services and authentication functions. Continuously hunt for signs of compromise or credential misuse, particularly in cloud environments.



Disable external management capabilities and set up an out-of-band management network.



Adopt a mindset that compromise happens: Prepare for incident response activities.



Block obsolete or unused protocols at the network edge and disable them in client device configurations.



For more information on how to mitigate the vulnerabilities and techniques the Russian Foreign Intelligence Service used, refer to the NSA, CISA and FBI advisory "Russian SVR Targets U.S. and Allied Networks" on [NSA.gov/cybersecurity-guidance](https://www.nsa.gov/cybersecurity-guidance).