# How Should You Respond to Russian Hacking Threat via MFA?

Author: Roy Hammett

---


As we enter a period of increased risk of cyber-attack, this article in Computing highlights again some items that database administrators and information security teams should consider, if they haven't done so already.

Organisations are being urged by federal agencies to immediately apply recommended mitigations to secure their machines.

The article states that the US Cybersecurity and Infrastructure Security Agency (CISA) and FBI have issued a joint security alert, urging organisations to immediately take steps to prevent Russian state-backed hackers from exploiting vulnerabilities in multifactor authentication (MFA) protocols and the Windows print spooler.

As per the advisory, an unnamed NGO's cloud and mail accounts were recently hacked by Russian actors who exploited MFA defaults and the critical '*PrintNightmare*' bug to steal sensitive information.

The victim's account had been un-enrolled from Duo owing to a prolonged period of inactivity but was not disabled in Active Directory. The hackers gained access to the network using a password guessing attack which was made possible by the victim's use of a simple and predictable password.

The hackers were able to add a new device to the account, satisfy the authentication requirements, and get access to the victim network - all allowed under Duo's default configuration settings, even for inactive accounts.

To cut a long story short – exploiting the *PrintNightmare* vulnerability (CVE-2021-34527) to gain administrator privileges and turn off MFA, the hackers were able to access confidential information.

Whilst the advisory focuses mainly on the risks to U.S. cleared defence contractors that have been targeted by Russian state-sponsored cyber actors, all commercial enterprises should be on notice that such attacks may occur.

For those managing data warehouses, we offer this advice:

1. Leaving dormant users with active database permissions is a bad thing, and can result in security breaches and data leaks, particularly if password security best practice is not followed.
2. Using Active Directory to manage all users across the entire enterprise consistently can help prevent such security breaches
3. Synchronising database users, groups, and permissions automatically with Active Directory can reduce the risks of a breach as compared with separate, manual database security management

For those managing Netezza databases, for example, there is a way of automating synchronisation with Active Directory using SmartSecure. More information can be found at https://smart-associates.biz/solutions/SmartSecure.php.



| Smart Associates (Aotearoa) Ltd | Smart Associates Ltd | Smart Associates ApS |
|---|---|---|
| 203/11 Vinegar Lane<br>Grey Lynne<br>Auckland 1021<br>New Zealand | Valley View, The Old Quarry<br>Haslemere<br>Surrey GU27 3SS<br>United Kingdom | % 360 Law Firm<br>Lautrupsgade 7, 3. tv<br>DK-2100 København Ø<br>Copenhagen, Denmark |
| T: +64 (9) 415-8120 | T: +44 (208) 133-6008 | T: +45 36 98 71 11 |