

# UK and Republic of Korea issue warning about DPRK state-linked cyber actors attacking software supply chains

Joint advisory observes cyber actors leveraging zero-day vulnerabilities and exploits in third-party software.

- New joint advisory describes techniques and tactics used by DPRK state-linked cyber actors carrying out software supply chain attacks
- UK's National Cyber Security Centre and Republic of Korea's National Intelligence Service warn that such attacks are growing in sophistication and volume
- Organisations are encouraged to put security measures in place to reduce the chance of systems and data being compromised

Cyber actors linked to the Democratic People's Republic of Korea (DPRK) are increasingly targeting software supply chain products to attack organisations around the world, the UK and the Republic of Korea have warned today (Thursday).

In a [new joint advisory](#), the National Cyber Security Centre (NCSC) – a part of GCHQ – and the National Intelligence Service (NIS) have detailed how DPRK state-linked cyber actors have been using increasingly sophisticated techniques to gain access to victims' systems.

The actors have been observed leveraging zero-day vulnerabilities and exploits in third-party software to gain access to specific targets or indiscriminate organisations via their supply chains.

The NCSC and the NIS consider these supply chain attacks to align and considerably help fulfil wider DPRK-state priorities, including revenue generation, espionage and the theft of advanced technologies.

The advisory provides technical details about the malicious activity, case studies of recent attacks emanating from the DPRK and advice on how organisations can mitigate supply chain compromises.

The publication follows the announcement of a new Strategic Cyber Partnership between the UK and the Republic of Korea, signed yesterday as part of a [landmark new Accord](#), which sees the two nations commit to working together to tackle common cyber threats.

**Paul Chichester, NCSC Director of Operations** said:

“In an increasingly digital and interconnected world, software supply chain attacks can have profound, far-reaching consequences for impacted organisations.

“Today, with our partners in the Republic of Korea, we have issued a warning about the growing threat from DPRK state-linked cyber actors carrying out such attacks with increasing sophistication.

“We strongly encourage organisations to follow the mitigative actions in the advisory to improve their resilience to supply chain attacks and reduce the risk of compromise.”

Software supply chain cyber attacks pose a significant threat as they can affect a number of organisations via one initial compromise and can lead to onward attacks, resulting in disruption or ransomware being deployed.

They can also be harder for network defenders to detect, as the actors are using legitimate software and hardware to enable the attack.

The advisory warns that the threat from DPRK state-linked actors carrying out these attacks is likely to increase and so organisations should follow the recommended actions to take to protect themselves.

This includes referring to the NCSC's [supply chain security guidance](#) for advice on how to establish effective control and

oversight of your supply chain.

[The full advisory can be read on the website of the Republic of Korea’s National Intelligence Service](#)

**PUBLISHED**

23 November 2023

**WRITTEN FOR**

Cyber security professionals

Large organisations

Public sector

Small & medium sized organisations

**NEWS TYPE**

Alert