

No follow-up on ransom demand

Cyber attack on South African weather service goes unnoticed

A cyber attack on the South African Weather Service on 26 January 2025 by an outfit identified as RansomHub has barely been noticed by the fresh produce sector. Not a single farmer or production manager approached by FreshPlaza was aware that South Africa's national meteorological service had been hacked.

The weather service announced the cyber attack the next day, noting "[it was] the second in the space of two days after the initial attempt on Saturday, 25 January 2025 failed".

For the three weeks between 26 January and 19 February, their central computer system was not in contact with its satellite weather stations, and the weather forecast models on which users rely for accurate weather forecasts, were in fact running on extrapolated data.

There are fears that climate data amassed since the early twentieth century could possibly be lost behind impenetrable encryption set in place by the hackers, who reportedly threatened to publish the hacked data on the dark web. It could, postulate industry-watchers, affect the weather service's ability to produce seasonal forecasts.

The hackers issued a ransom note but, remarks Oupa Segalwe, chief communications officer at the South African Weather Service, "there was no specificity with respect to the ransom amount. No follow-up has been made by the hackers either." The weather service is trying to recover its databases and a criminal case has since been opened with the South African Police Service.

Website back online with limited functionality

The SAWS website was offline for almost a month and still has limited functionality: historical rainfall, synoptic charts, and recent climate data are not yet available.

"The public can now access daily rainfall, minimum and maximum weather temperature forecasts, as well as severe weather warnings via the SAWS's main website, amongst other currently used avenues of access," Ishaam Abader, CEO of the South African Weather Service explains in a press release issued this week.



A Western Cape citrus orchard under a blanket of winter snow (photo used as illustration only)

Models keep running in absence of new data

Since the cyber attack, there has been an interruption in receiving upper-air data (which is being set right now). "You can infer from satellite imagery but if you don't have upper air data, the models will most definitely be compromised," says a member of the meteorological community on condition of anonymity.

Fruit farmers use weather forecasts to plan their irrigation, chemical applications, and harvesting. A number of the same names crop up among South African fruit farmers when asked about their source of weather information: yr.no, Accuweather, windy.com, Vox, Ventusky. None named the South African Weather Service as their primary source of weather information.

However, weather-watchers are all dependent on the South African weather service even if they don't use it directly. All commercial weather apps obtain their input from the primary data collected and relayed by South Africa to meteorological services in the UK and the USA.

Because there have been no severe weather events – it's high summer, therefore the interior expects afternoon thunderstorms and the coast is under the influence of high pressure – the disruption in services didn't attract wide notice.

SAWS warned ahead of recent disruptive rainfall

Fortuitously on 16 February 2025, the weather service was able to warn of the disruptive rainfall over southwestern Africa which has since caused nine deaths in Botswana, six in Durban yesterday, and widespread flooding. FreshPlaza has reported on the impact of this rainfall on vegetable production

(<https://www.freshplaza.com/africa/article/9708352/after-deluge-quick-rise-in-tomato-prices-will-circle-out-to-all-veg-lines/>).



Exactly two years ago: an inundated sugarcane field in Mozambique after Tropical Cyclone Freddy, the longest-living tropical storm anywhere on record. The South African Weather Service's functionality also affects millions in its neighbouring countries

Forecast product generating system back in operation

The weather service relies on "a comprehensive suite of Numerical Weather Prediction (NWP) models, primarily based on the Unified Model from the UK Met Office", supported by others, to generate short-range weather forecasts and warnings. "Despite the manual aspects of some operational procedures, the SAWS' forecasts have demonstrated high reliability, as is evident from the recent flood warnings and daily forecasts that were issued by the SAWS," the weather service replied to FreshPlaza's questions.

The weather service has restored contact with its weather stations and its forecast product generating system was brought back into operation on 25 February 2025, enabling the digital transmission of weather products, including forecasts, alerts, and warnings.

Members of the meteorological community call the cyber attack a national disaster. "One day of lost data is a disaster as far as I'm concerned."



For more information

South African Weather Service

Tel: +2712 367 6111

Email: Oupa.Segalwe@weathersa.co.za

<https://www.weathersa.co.za/> (<https://www.weathersa.co.za/>)

Publication date: Mon 3 Mar 2025

© FreshPlaza.com / Carolize Jansen

•

