CVE-2022-26493 - miniOrange SAML

In March of 2022, miniOrange publicly released the latest versions of our Drupal SAML SP Modules.
This latest version of the module, patches a security vulnerability that was found during testing, that allowed the attacker to get unauthorized access to the website.

What it was:
The vulnerability was around the signature verification in the SAML SSO flow. If the response was signed, then it was subject to verification.
However, if it was unsigned, the verification was skipped and the user was logged in.

How it could be exploited:
If one could sniff a signed SAML response, remove the signature, followed by replacing the username in the SAML response by the username of an existing user in the Drupal user base, then, theoretically, they could have been able to gain access to the website by logging into the user's account specified in the infected response.

This vulnerability was caught early and has since been patched in the module versions more than or equal to the list below. (**The community version of the module available on the Drupal marketplace was not affected with this vulnerability**)

Drupal 8 / Drupal 9		Drupal 7	
Module Variant	Patched Version	Module Variant	Patched Variant
Standard	20.3	Standard	20.2

Premium	30.5	Premium	30.2
Enterprise	40.4	Enterprise	40.2

If you are using an out-dated/ vulnerable version of the SAML SP module, you can download the latest version by signing in to your miniOrange dashboard using the registered credentials.

We would like to thank **Robert Farmer** and the team from **Semantic Bits**, for pointing out this vulnerability.