Click Studios
ABN: 84 321 815 001

Level 3, 97 Pirie St
Adelaide, SA, 5000
Australia

Phone:+61 88120 0630

sales@clickstudios.com.au
www.clickstudios.com.au

clickstudios PASSWORDSTATE

INCIDENT MANAGEMENT ADVISORY #01

Dated: 3rd June 2022, 1:45 PM (Australian CDT)

Click Studios advises it has worked with DigiCert to revoke the digital signing certificate used to sign our software and obtain a replacement. We have taken this action based on analysis of malware discovered to have been signed by a copy of our SHA 256 Digital Certificate.

Advisory Summary:
Click Studios has been approached by an Anti-Virus company, advising analysis of some copies of malware involved in the **exploitation of Microsoft Office zero-day vulnerability "Follina"**, appear to be digitally signed with a copy of the Click Studios DigiCert SHA 256 Digital Certificate. While no Passwordstate code or functionality has been directly targeted or affected we have requested DigiCert to revoke the certificate. **Once revoked your Passwordstate instances availability may be impacted through operating system, antivirus, or endpoint protection software.**

Analysis:
On 2nd June 2022 at 12:23 PM Australian CDT an Anti-Virus Software provider contacted Click Studios Technical Support. They advised some copies of malware, involved in the exploitation of the **"Follina" zero-day vulnerability in the Microsoft Support Diagnostic Tool (CVE-2022-30190),** appeared to be signed by Click Studios DigiCert SHA 256 Digital Certificate.

This certificate is used to digitally sign DLLs, Executables and Installers, confirming the software has not been altered or corrupted since it was signed. It does this through the use of a cryptographic hash to validate authenticity and integrity.

At this stage it is not known how a copy of the Click Studios DigiCert SHA 256 Digital Certificate has been obtained.

Remedial Actions:
Click Studios has officially invoked its Incident Management Plan **and the number one priority is to shut down any attempt to digitally sign software not originating from Click Studios**.

Digital Certificate Revocation is used to prevent the spread of malware and address system-wide attacks and vulnerabilities. As a member of the online community Click Studios cannot allow a copy of our DigiCert SHA 256 Digital Certificate to be used to digitally sign malware. This has required working with DigiCert to request revocation of the existing certificate and have obtained a new certificate.

Our development team has signed binaries and assemblies with the new certificate and recompiled the Passwordstate software. Updated installers are now available via the link below
https://www.clickstudios.com.au/passwordstate-checksums.aspx

Request for Additional Information:
Requests for information, clarification, and updated analysis will only be provided via these Incident Management Advisories. All Email requests from customers on updated information relating to this incident, or from the Media, will be directed to the Incident Management Advisories posted on our website.

These are the only authorized updates as per our Incident Management process. If customers are unsure of the validity of an email we have sent them, they should send it to Technical Support as an attachment, for confirmation.