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 #02

Dated: 4th June 2022, 10:30 AM (Australian CDT)

Click Studios advises it has worked with DigiCert to revoke the digital signing certificate used to sign our software. A new certificate has been obtained, used and new builds of Passwordstate have been released. 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.**

Reading Incident Management Advisories:
Click Studios Advisories are accumulative with each update building on previous advisories content. Duplication of content is only included to reiterate facts and requests or where information has changed.

Updated Status:
On 2nd June 2022 at 12:23 PM (ACDT) 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.

The Revocation request was submitted to DigiCert on 2nd June 2022 at 2:35 PM (ACDT). A new DigiCert SHA 384 Digital Certificate, Serial Number 0894fb6216c1f6dc4d1584c07f628a4d has been obtained and used to sign new Passwordstate Builds 8995 and 9535. All Nominated Contacts have been emailed advising to upgrade to the latest builds.

On 2nd June 2022 at 01:45 PM (ACDT) the Root Cause Analysis Team was formed and commenced planning the review of code, downloads and systems access. **At this stage it is not known how a copy of the Click Studios DigiCert SHA 256 Digital Certificate has been obtained.**

Why Have We Taken This Action:
Click Studios cannot allow a copy of our DigiCert SHA 256 Digital Certificate to be used to digitally sign any software not originating from us. The only means of preventing this, as confirmed via our DigiCert Support Call, is by revoking that certificate. The request to revoke the affected certificate was submitted 2nd June 2022 at 2:35 PM (ACDT). **Its status is currently pending DigiCert's investigation.**

Passwordstate Has Not Been Manipulated:
To the best of our knowledge Passwordstate has not been manipulated. The Root Cause Analysis team has performed a detailed code review, checked ZIPs and compared checksum values. There is no evidence of tampering with software available from Click Studios website and controlled CDN Network.

There are no reports of malware currently targeting Passwordstate. The malware signed with a copy of Click Studios DigiCert SHA 256 Digital Certificate relates to the Microsoft Office zero-day vulnerability stated above.

What Happens To Previously Signed Versions Once Revocation Has Occurred:
The following builds of Passwordstate will be affected by the revocation of the certificate,

- **Passwordstate Version 8, Builds 8987 through 8995**, and,
- **Passwordstate V9, all builds**

Builds prior to Version 8, 8987 were signed with an older certificate which has now expired. That digital certificate cannot be used to digitally sign new code.

To the best of our knowledge any Passwordstate instance affected by the revocation of the digital certificate, that is internet accessible, will be impacted by your operating system, antivirus, or endpoint protection software not trusting the Passwordstate Software and warning or preventing its ability to load and run. **This is yet to be tested as the DigiCert revocation request is currently pending DigiCert's investigation.**

How Has This Happened:
The Root Cause Analysis Team has completed the following reviews.

- Code reviews – no issues,
- Build delivery ZIP packages and matching checksum values – no issues
- DigiCert portal access against audit records, IP addresses and date stamps - no issues
- Click Studios perimeter network logs and access to development LAN – no issues

While there is no evidence, that Click Studios network or development LAN are currently compromised, we have commenced discussions with a specialist 3rd Party provider for validation.

Request for Additional Information:
Reports outside of these Incident Management Advisories should not be taken as authoritative. These published updates are the only authorized source of information as per our Incident Management process.

All requests for information are directed to our Advisories webpage, where advisories will detail all known facts, including any Passwordstate functionality that has been compromised. **If we have not explicitly stated that functionality is compromised then it is safe to use**.