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 #03

Dated: 7th June 2022, 11:45 AM (Australian CST)

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 were advised by an Anti-Virus company that 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. No Passwordstate code or functionality has been directly targeted or affected. DigiCert have been requested to revoke the affected certificate and the status is pending their investigation. Root Cause Analysis has completed with two anomalies found.

Once DigiCert revoke the affected certificate your Passwordstate instances availability may be impacted through operating system, antivirus, or endpoint protection software.

Updated Status:
Advisories #01 and #02 incorrectly state the time was Australian CDT. While the times stated are correct, they are in Australian CST (Central Standard Time).

An Anti-Virus Software provider contacted Click Studios Technical Support advising 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 request submitted to DigiCert on 2nd June 2022 at 2:35 PM (ACST) to revoke the affected certificate is still pending their investigation. Click Studios has stressed the importance of revoking the old certificate and DigiCert have internally escalated the request.

Root Cause Analysis Findings:
As previous advised, the Root Cause Analysis Team has completed reviews related to,

- 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.

The following reviews have also now been completed,

- Patch reviews for all systems – no issues,
- Microsoft Exchange Server scans for compromises – no issues,
- Detailed full scans of all LANs Servers and Computers – no issues,
- Full review of access to Website, Blog and Forum sites – no issues,
- Full review of Source Control Logs – **2 (two) anomalies discovered**.

Based on the internal reviews conducted there are currently no known compromises to Passwordstate, Click Studios network, the public facing website or blog and forum sites. We are currently in discussion with a specialist 3rd Party provider for validation that networks and websites are consistent with internal findings.

Source Control Log Anomalies:
Click Studios historically used a process of manually building Upload Packages for our public facing website content changes. They only included updated website pages and published PDFs.

The application of Upload Packages worked on a comparison basis with discrepancies flagged when a corresponding file didn't exist in either the originating source or target destination.

The Source Control Log anomalies relate to 2 Upload Packages. On 29th March 2021 a copy of the DigiCert SHA 256 Digital Certificate was inadvertently included in an Upload Package. This coincided with the release of Passwordstate 9.1 Build 9100. While the discrepancy, relating to the file not existing in the target destination was flagged in the Source Control Log, the issues was either missed or not escalated.

On the 14th April 2021, the Upload Package coinciding with the release of Passwordstate 9.1 Build 9112, flagged in the Source Control Log the DigiCert SHA 256 Digital Certificate didn't exist in the originating source. The employee performing the processing of both Upload Packages realized the mistake and manually deleted the DigiCert SHA 256 Digital Certificate from the public facing website. While they attempted to fix the issue, it was not escalated to Line Management.

Based on the above, it is believed the source of the compromised DigiCert SHA 256 Digital Certificate was the old public facing website. The timing of these events occurred prior to the compromise to the upgrade director located on the website between 20th April 2021 8:33 PM UTC and 22nd April 2021 0:30 AM UTC.

Improved Change Control Introduced with Build 9300:
Click Studios introduced multiple improvements to our Change Control processes coinciding with the release of Passwordstate 9.3 Build 9300 on 2nd August 2021. These improved processes apply to all releases of Software and website changes. They include improved product lifecycle tracking tools, 2 stage peer reviews, and independent gate approver between Development, Quality Assurance and Production environment migrations.

Liaison with the Australian Cyber Security Centre:
The ACSC (Australian Cyber Security Centre) is aware and has been briefed by Click Studios. Any Australian organizations that believe they have been affected by the "Follina" zero-day vulnerability in the Microsoft Support Diagnostic Tool (CVE-2022-30190) signed by Click Studios DigiCert SHA 256 Digital Certificate, should contact them via ASD.Assist@defence.gov.au or 1300 CYBER1.

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**.