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: 25th April 2021, 9:40 AM (Australian CDT)

Click Studios advises that any customer that has performed an In-Place Upgrade between 20th April 2021 8:33 PM UTC and 22nd April 2021 0:30 AM UTC had the potential to download a malformed Passwordstate_upgrade.zip file.

Advisory Summary:
As stated in **Incident Management Advisory #01**, the best information we have relating to the number of affected customers is based on the 28 hour window of opportunity, the nature of the initial compromise and subsequent exploit, and customers provision of information. The number of affected customers still appears to be very low, however this may change as more customers supply the requested information. Only customers that performed In-Place Upgrades between the times stated above are believed to be affected and may have had their Passwordstate password records harvested.

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 Analysis:
A leading cybersecurity company have released an advisory, the details of which supports Click Studios initial analysis. A copy of this was provided to Click Studios, however it is for internal use and Click Studios has been requested to not share it at this time. As previously reported the following fields in Passwordstate instance's password table is posted back:

Title, UserName, Description, GenericField1, GenericField2, GenericField3, Notes, URL, Password

However, if customers had selected to encrypt the GenericFields above then information in these GenericFields would not have been harvested and posted to the bad actor CDN network.

Customers wanting to confirm their installations Moserware.SecretSplitter.dll is unaffected can do so by confirming the checksums of the file, located in c:\inetpub\passwordstate\bin\ against the following;

- **File size = 61KB**
- **MD5 Checksum = 12446D738BDD6B7A61B3A823F608AE7F**
- **SHA1 Checksum = 774B5F05C8E538E2FE7F451C55782E43DC103530**
- **SHA256 Checksum = 1EE0F14C44058E3D0D1C19B4713D573C81B49C28ED58BD41C72832C78F7D1464**

To be clear, Click Studios CDN Network was not compromised. The initial compromise pointed the In-Place Upgrade functionality to a CDN network not controlled by Click Studios.

Identification and Remedial Actions:
Click Studios number one priority is working with our customers, identifying if they have been affected and advising them of the required remedial actions. It is essential that customers follow the instructions provided in Incident Management Advisory #01 and subsequent emails received from Click Studios.

Request for Additional Information:
Reports of the incident in traditional or social media should not be taken as authoritative. The Incident Management Advisories are the only authorized updates 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**.