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 #04

Dated: 28th April 2021, 10:40 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:
The number of affected customers is still very low. Only customers that performed In-Place Upgrades between the times stated above are believed to be affected. Customers are requested not to post Click Studios correspondence on Social Media. It is expected that the bad actor is actively monitoring Social Media, looking for information they can use to their advantage, for related attacks.

Posting of Click Studios Emails on Social Media:
Customers were sent an email, subject: Confirmation of Malformed Files and Essential Course of Action on Friday 23rd at 1:41PM ACDT. Unfortunately, some customers have posted copies of this email on social media. It is expected the bad actor is actively monitoring social media for information on the compromise and exploit. It is important customers do not post information on Social Media that can be used by the bad actor. This has happened with phishing emails being sent that replicate Click Studios email content.

Customers Reporting Phishing Attacks:
We have been advised a bad actor has commenced a phishing attack with a small number of customers having received emails requesting urgent action. These emails are not sent by Click Studios and can be confirmed as not legitimate by;

- **The sending email has a strange domain suffix** - (note this may change over time)
- **Wording - Urgent there is a bug in the last upgrade, you have to download another file to overwrite it**
- **The download location is a subdomain**
- **The checksum provided is not legitimate for our software**

Customers are reminded to stay vigilant and ensure the validity of any email sent to them. If you are unsure if an email is from us, send it to Technical Support as an attachment, for confirmation.

Initial Analysis of Phishing Attack:
The phishing attack is requesting customers to download a modified hotfix Moserware.zip file, from a CDN Network not controlled by Click Studios, that now appears to have been taken down. Initial analysis indicates this has a newly modified version of the malformed Moserware.SecretSplitter.dll, that on loading then attempts to use an alternate site to obtain the payload file. We are still analysing this payload file.

Identification, Remedial Actions and Advice:
Click Studios number one priority is working with our customers, identifying if they have been affected and advising them of the required remedial actions. The **ACSC (Australian Cyber Security Centre)** is aware of the incident, providing advice to Click Studios. Any Australian organizations that believe they have been affected should contact them via ASD.Assist@defence.gov.au or 1300 CYBER1.

Request for Additional Information:
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**.