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: 24th April 2021, 12:38 PM (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:
Initial analysis indicates that a bad actor using sophisticated techniques compromised the In-Place Upgrade functionality. The initial compromise was made to the upgrade director located on Click Studios website www.clickstudios.com.au. The upgrade director points the In-Place Upgrade to the appropriate version of software located on the Content Distribution Network. The compromise existed for approximately 28 hours before it was closed down. Only customers that performed In-Place Upgrades between the times stated above are believed to be affected. Manual Upgrades of Passwordstate are not compromised. Affected customers password records may have been harvested.

Analysis:
The initial compromise of the director file located on Click Studios website www.clickstudios.com.au is not attributed to stolen or weak credentials.

Any In-Place Upgrades performed between 20th April 8:33 PM UTC and 22nd April 0:30 AM UTC have the potential to download a malformed Passwordstate_upgrade.zip. This .zip file was sourced from a download network not controlled by Click Studios.

When the In-Place Upgrade capability processes the malformed Passwordstate_upgrade.zip a modified moserware.secretsplitter.dll, with a size of 65kb, is loaded. This subsequently downloads an additional file upgrade_service_upgrade.zip file from a bad actors CDN network, starts a new background thread, converts the upgrade_service_upgrade.zip to a .NET assembly only stored in memory and begins processing.

The process extracts information about the computer system, and selects Passwordstate data, which is then posted to the bad actors CDN network. On completion the thread is then slept for 1 day.

Analysis of compromised data indicates the following information is posted back:

> **Computer Name, User Name, Domain Name, Current Process Name, Current Process Id, All running Processes name and ID, All running services name, display name and status, Passwordstate instance's Proxy Server Address, Username and Password**

The following fields in Passwordstate instance's password table is posted back:

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

The Domain Name and Host name aren't extracted as part of this. Although the encryption key and database connection string are used to process data via hooking into the Passwordstate Service process, there is no evidence of encryption keys or database connection strings being posted to the bad actor CDN network.

Identification and Remedial Actions:
Click Studios number one priority is preventing the compromise from continuing to be exploited and to work with our customers, identifying if they have been affected and advising them of the required remedial actions.

Customers have been advised to check the file size of moserware.secretsplitter.dll located in their c:\inetpub\passwordstate\bin\ directory. If the file size is 65kb then they are likely to have been affected. They are requested to contact Click Studios with a directory listing of c:\inetpub\passwordstate\bin output to a file called PasswordstateBin.txt and send this to Click Studios Technical Support.

Affected customers are then advised by Click Studios Technical Support via email to;

1. **Download the advised hotfix file**
2. **Use PowerShell to confirm the checksum of the hotfix file matches the details supplied**
3. **Stop the Passwordstate Service and Internet Information Server**
4. **Extract the hotfix to the specified folder**
5. **Restart the Passwordstate Service, and Internet Information Server**

Once this is done it is important that customers commence resetting all Passwords contained within Passwordstate. These may have been posted to the bad actors CDN network. Click Studios recommends prioritizing resets based on the following;

1. **All credentials for externally facing systems, i.e., Firewalls, VPN, external websites etc.**
2. **All credentials for internal infrastructure, i.e., Switches, Storage Systems, Local Accounts**
3. **All remaining credentials stored in Passwordstate**

High Level Summary of what we have done:
Click Studios treats this issue seriously and invoked our Incident Management Plan on the evening of 21st April (ACDT).

Our initial focus was to work with the small number of customers who were reporting issues with In-Place Upgrades. On the morning of 22nd April (ACDT) we successfully replicated the issue on an isolated test machine, and at 10:00 AM (ACDT), blocked the ability for customers In-Place Upgrades to work. We reached out to our hosting company and partner CDN network for relevant logfiles and more information.

In-house Senior Developers, Technical and Security staff then commenced detailed analysis of the isolated test machine. Once initial analysis was sufficiently advanced, and we understood the nature of the compromise, and the timeframe the comprise was available to be exploited, we emailed all know active customers via their nominated contacts. This email was sent on 22nd April 20:56 (ACDT).

Click Studios is continuing to work with our customers, identifying if they have been affected and advising them of the required remedial actions. Click Studios is also liaising with a Nationally Based 3rd party for assistance on in-depth analysis and direction for specialist technical support.

Level of Exposure:
Click Studios has an extensive Global Customer base. The best information we have relating to the number of affected customers is based on the window of opportunity, approximately 28 hours, the nature of the initial compromise and subsequent exploit, and customers provision of requested information. **At his stage the number of affected customers appears to be very low. However, this may change as more customers supply the requested information**.

Request for Additional Information:
Click Studios is understandably being requested for additional information by existing and potential customers, the media and other parties. As stated previously in this advisory, our number one priority is working with our customers, identifying if they have been affected and advising them of the required remedial actions. 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.

Requests for information, clarification on the level of exposure 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.