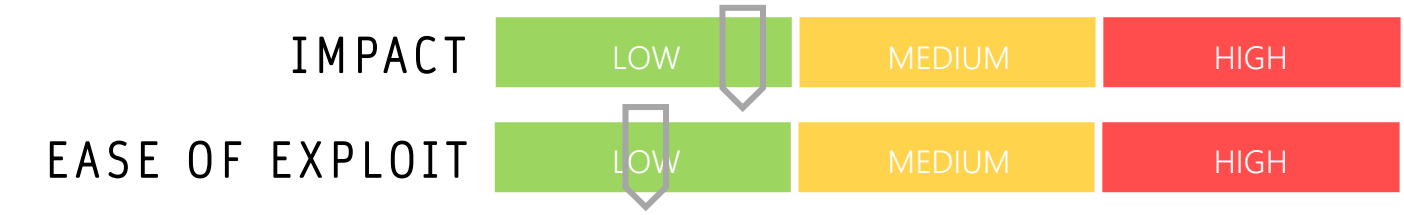
UNISPHERE SOLUTIONS
info@unisphere.co.nz
www.unisphere.co.nz

CYBER GUIDANCE ISSUE 00015

ANCESTRY.COM DATA LEAK

DATE ISSUED: 22nd July 2020



OVERVIEW

The 'Family Tree Maker' software utilised by ancestry.com that synchronises with user's family history data in connection with an open and unencrypted ElasticSearch Server maintained by Software MacKiev has recently had a leak discovered that may jeopardise the privacy of up to 60,000 users of the genealogy site.

BREAKDOWN

A misconfiguration of the ElasticSearch server appears to be the culprit of the leaked information, which includes users email addresses, location data, technical support communications and other technical data. Such a leak has the potential to expose users to phishing, fraud and even identity theft. The database has since been secured after Software MacKiev received information regarding the potential breach from the WizCase research lab.

This breach highlights the importance of securing and maintaining the security of data stored on the cloud which may include measures such as encryption. A data-centric approach relies on not only securing the borders but rather to protect the data through the enforcement of the appropriate policies to secure the data at all stages, including in use, throughout transmission and at rest.

REMEDIATION STEPS

- Remain vigilant for phishing and verify email authenticity through visual and/or technical analysis
- Investigate use of Ancestry.com on company devices and take appropriate actions where necessary

REFERENCES & RESOURCES

Threatpost: https://threatpost.com/leak-exposes-private-data-of-genealogy-service-users/157612/