Waterstons
we're with you

+44 345 094 0945
www.waterstons.com

News article

May 2024

Microsoft Internal Files Accidentally Exposed to The Internet

An improperly configured server has left internal Microsoft data, including passwords, exposed online.

Craig Archdeacon
Director - APAC
Email craig.archdeacon@waterstons.com

What happened

On February 6th, security researchers discovered that an internal Microsoft storage server, hosted within Azure, was publicly accessible online. The server did not require any authentication, exposing the sensitive data to anyone who found it. The server contained data related to Microsoft's Bing search engine, including code, scripts, and configuration files, some of which contained credentials and keys for internal systems.

The exposed server was reported to Microsoft on February 6th however, it was only secured on March 5th - almost a month later. It is unknown how long the server was exposed for prior to discovery. It is also not clear if any threat actors had accessed the data.

Following the incident Microsoft has stated that the credentials stored within the server were temporary, had been disabled, and were related to systems only accessible via the internal network. However, the data could be used to help craft future attacks if accessed by threat actors.

Wider implications

This incident highlights that accidental data exposure can pose just as significant a risk as malicious threat actors. Cyber security is not just about preventing threat actors from exploiting vulnerabilities or carrying out social engineering attacks, but also about securely configuring an organisation's internal environment, minimising access to only those who require it.

Even if the data involved is not directly damaging to the organisation or any individuals, as it appears in this incident, it could be used to craft more sophisticated and effective attacks in the future. Any internal-only information that is revealed could be used by threat actors to gain a better understanding of an organisations internal environment or conduct more sophisticated and targeted social engineering attack.

Organisations should:

- Ensure they develop and implement secure configuration standards for new devices, requiring default passwords to be reset when new devices/applications are deployed in the IT environment. Where appropriate, organisations should align with industry standard benchmarks, such as the Centre for Internet Security (CIS).
- Conduct regular vulnerability assessments and penetration tests to identify and remediate any improperly configured, or internet-exposed, devices before they are exposed to cyberattacks.
- Ensure that credentials are not stored in plaintext to minimise the impact if they are stolen in a data breach.
- Ensure all account credentials, particularly privileged accounts, are disabled as soon as they are no longer required to minimise the risk of account compromise.

This article and other fantastic insights are shared in our monthly cyber threat report. You can join the mailing list to receive it here.

Waterstons has 25+ years' experience across the UK and Australia preparing and protection organisations from cyber threats. We are committed to assisting all organisations to stay agile and prepared in today’s cyber conscious economy.

Empower your organisation today, get in touch with one of our team members.

info@waterstons.com.au I 02 9160 8430