CYBERSECURITY POLICY AND INCIDENTS BRIEFING

INTELLIGENT BUILDINGS℠

ICYMI: Intelligent Buildings spotlights how a Chinese-speaking threat actor attacked building automation systems in several Asian countries using a Microsoft Exchange vulnerability

06/30/22

SUMMARY

Attacks were launched against building automation systems in several Asian organizations to gain access to more secure areas of their networks. They used Microsoft Exchange vulnerabilities known as ProxyLogon. The ProxyLogon attack can be used against unpatched mail servers running Microsoft Exchange Server 2013, 2016, or 2019 that are set up to receive untrusted connections from the outside world. This enables threat actors to execute commands on unpatched, on-premises Exchange Servers. The threat actors used this to access even more secure areas of the network, allowing them to collect previously protected data and information that is likely damaging to the company.

WHAT IT MEANS

ProxyLogon is a pre-authenticated vulnerability, meaning an attacker doesn't need to log on or complete any authentication process to execute code remotely. Even though Microsoft released the patch, sources such as DIVD say that at least 46,000 servers are still unpatched and vulnerable to ProxyLogon flaws. Last year, ESET said that at least ten hacking groups were using ProxyLogon exploits way before Microsoft released patches last spring, so even if a system is updated now with the patch, it may have been compromised by threat actors using ProxyLogon prior to the update.

Most building owners have an incomplete/inaccurate understanding of all the systems in their portfolios. In our experience, many building owners often underestimate the number of internet-connected devices and systems in their buildings. Internet connections are gateways for bad actors to access your network. This is why real-time, continual monitoring of your systems is critical.

You can prepare by:

- Using building system network traffic monitoring, analysis, and detection
- Updating operating systems regularly
- Applying security fixes and patches as soon as reasonably possible
- Conducting regular security audits to identify vulnerabilities and eliminate them
- Conducting building cybersecurity training that includes threat awareness and familiarization with cybersecurity practices

HOW INTELLIGENT BUILDINGS CAN HELP

We have assessed thousands of buildings in the US, Canada, and overseas. In our experience, most building owners don't know what's connected or how it's connected and configured, and do not have recovery strategies in place. For example, even if backups are being performed, they are usually not being performed correctly or securely. Intelligent Buildings can **assess your building systems and the contractors** who support them to provide you with an easy-to-follow plan to secure your building control systems. Further, our managed service helps to ensure these steps are being followed and that y**our systems, cyber risks and contractor processes are bought into compliance**.

For more information about this incident and other news, contact us at info@intelligentbuildings.com