Cyber Update: Microsoft Exchange server vulnerability

The specialist Cyber team at Crawford & Company® continues to successfully manage significant levels of new instructions in relation to the Microsoft Exchange server vulnerability. First hand we are seeing evidence of the anticipated second wave of attacks, whereby advanced persistent threat groups are now taking advantage of the well-publicized security flaw, seeking to exploit and monetize the gap at the expense of insureds.

The Crawford® Cyber team has imported their experience in Cyber incident response, loss handling and surge planning, utilizing the strength and depth of their resources and their contracted vendor network. As a benefit of having a truly global offering, they have ensured continued and consistent available capacity to safeguard service levels, attesting that the team remains best placed to be able to respond.

How did we get here?

In the first few days in March 2021, Microsoft issued an advisory, releasing multiple security patches to address vulnerabilities in their Microsoft Exchange e-mail server operating system, which had been allowing attacks to on-site e-mail servers.

It was identified that four of the most dangerous vulnerabilities were already being exploited, which granted attackers the ability to deploy a three-stage attack. Firstly, the attacker accesses an Exchange server, using privileged access to monitor the IT environment, secondly they create a “web shell” which is a form of backdoor to permit remote server access, finally the threat actor utilizes the backdoor to steal data from the victim’s seemingly secure network. Microsoft announced these attacks were “limited and targeted”.

Evidentially, it is understood that these vulnerabilities have been exploited by State sponsored threat actors, potentially since November / December 2020. Primarily, it is believed their aim was to use espionage to monitor e-mail communications and steal sensitive, secretive or valuable data. The targets to date have been confined to amongst others; government departments, local authorities, ‘think tanks’, medical research groups, defence contractors, law firms and higher education institutions. It is widely believed by cyber security experts that the group may have infiltrated “hundreds of thousands” of Microsoft Exchange Servers worldwide.

Where are we now?

Since releasing the patches in early March, this has brought the vulnerabilities to the wider cybercriminal and dark-web community.

Subsequently creating a tidal wave of advanced persistent threat groups taking advantage of the known vulnerabilities and the delay in users installing the patches. Ultimately, their aim is much more sinister as they seek to harvest personal identifiable information for monetary gain, or worse, use the vulnerabilities to get a foothold in the user's IT network, either deploying ransomware or sending payment diversion e-mails. Such outcomes can be disastrous to a business, both in terms of immediate ability to function and trade, but also long term impacts with financial, reputational, regulatory and liability risks.

What can be done?

Users should coordinate with their internal IT departments and follow their instructions with regard to installing the patches as a priority.

Organizations also have the option to follow Microsoft's recommended steps in their blog: https://www.microsoft.com/security/blog/2021/03/02/hafnium-targeting-exchange-servers/#scan-log to confirm if they have been compromised.

Crawford's continued response

Alongside our ability to assemble cyber accredited experts across the globe on a 24/7 basis, we have engaged with our expert vendor panel to ensure a clear and defined process, allowing immediate response and assistance to:

Understand wider risks such as regulatory and legal;

Considering if there have been any prior compromises;

Immediate containment and securing of the IT environment, removing "backdoors" etc.; and

Full forensic analysis to confirm the degree and extent of compromise if warranted.

Importantly, a consistent and clearly defined approach will allow us to continue to provide a prompt response to assist the insured when they are at their most vulnerable and ultimately support insurers' interests with the effective management of the cost of the claim.

Alongside the immediate response needs, there will ultimately be a greater potential for either long term future risks, notably through the recent DEARCRY ransomware or 'after the event' notifications. Such 'after the event' losses require careful supervision and consideration, utilizing traditional loss adjusting expertise to manage insurers' outlay.

Crawford remain at the disposal of our clients to assist in the continued coordination and response to this cyber event, to include access to specialist Cyber loss adjusting and claims management services by way of supporting both immediate and future claims needs.

More information

For more information, please contact:

Paul Handy, BSc (Hons),
MBA, ACII, FCILA, FUEDI-ELAE, FIFAA, ACMI
Global Head of Cyber
T +44 7827 879 187
E: paul.handy@crawco.co.uk

About Crawford & Company®

For over 75 years, Crawford has solved the world's claims handling challenges and helped businesses keep their focus where it belongs – on people.

Loss Adjusting | Third Party Administration | Managed Repair | Medical Management | On-Demand Services | Catastrophe Response

9,000 employees | **50,000** field resources | **70** countries | **$18B** claims managed annually

Crawford®

CRAW-CYBER-SS-LETTER-WP-0321

Learn more at
www.crawco.com/services/cyber-risk