CYBERSPRINT
BREAKTHROUGH SECURITY

EDITORIAL

EXCHANGE CVEs

THE RESPONSE PLAN GAP THAT DOUBLED THE PATCHING EFFORT

BY **EWARD DRIEHUIS**
SVP STRATEGY CYBERSPRINT

EXCHANGE CVEs

THE RESPONSE PLAN GAP THAT DOUBLED THE PATCHING EFFORT

BY **E. DRIEHUIS**
SVP Strategy

It’s been two weeks since Microsoft released a patch[1] for the Exchange vulnerabilities. For many, the dust has settled. Others are still fighting fires. Today, I’d like to look back at some of the problems we saw.

However, timing is always an issue. It’s not my intention to jump on the bandwagon or engage in ‘ambulance chasing’ with this topic. I know the vulnerabilities had severe implications for some.

If you are still putting out fires, this[2] might be helpful. Or rather, look at the mitigations provided[3] by Microsoft. If you run Exchange on-prem and don’t know what all the commotion is about, I recommend you stop reading and google “exchange vulnerability” now - It’s critical.

With all of this out of the way, I’d like to share some of our takeaways and insights after having dived into the problem to help some organisations. These takeaways are by no means relevant to just the Exchange CVEs and apply to other zero-days, vulnerabilities, and even to broader incident response scenarios as well.

ON ZERO-DAYS AND THEIR IMPACT

The Exchange zero-day impacted a wide variety of organisations. It could be found and exploited remotely. The speed of scanning from the good guys and the bad guys alike was awe-inspiring. Experts I spoke with estimated the global IP space was scanned within hours. As bad as this is, it’s by no means unique. Over the last two years, we’ve seen several other bad incidents:

- Pulse Secure VPN released a fix for a remote exploit in April 2019. Yet, unpatched instances were still exploited[4] for deploying ransomware in 2020.
- The Citrix Netscaler vulnerabilities[5] lead to remote access functionalities being turned off while security experts waited for a patch. This actually resulted in massive traffic jams as everybody had to work at the office.

The recent SolarWind breaches were supply chain attacks rather than zero days. Semantics aside, the effect is the same.

The impact to any organisation is not to be underestimated, and the best mitigation in these situations is usually to ‘assume compromise’, which includes invoking an incident response process. Investigations typically need to focus beyond the affected machine since lateral movement (island hopping to the next machine) needs to be expected.

Estimates are that 90% of exposed servers have been infected. It means that an organisation is probably ‘on the shelf’ of the bad guys. Some of them have already been hit with DearCry[6].

INCIDENT RESPONSE AND ZERO-DAYS

A common perspective to incident response scenarios is through these six phases:

1. Prepare: think of the processes you need for each of the following phases, and train them. It will help you get through an actual incident as smoothly as possible.
2. Identify: where is your stuff and what is that stuff, and which parts of it are affected by the incident?
3. Contain: make sure it doesn't get any worse.
4. Eradicate: find and eliminate the root cause.
5. Recover: normalise the situation and move into production again.
6. Evaluate & improve: learn what you can do to avoid these issues in the future.

When a vulnerability incident happens, an organisation is catapulted into phase 2. Where can you find the affected infrastructure? Answers need to come in fast because response teams want to stop the bleeding in the *containment* phase as soon as possible. The focus needs to be on the assumption the attackers might have moved laterally. You need to investigate the affected infrastructure and the surrounding infrastructure alike.

COMMON ISSUES

In our work over the last weeks, we've observed and contributed to these processes. We have confirmed one of the common problems and noticed two new ones.

Preparing is everything: it is widely accepted that organisations need to invest more time preparing for incidents such as zero days. Studies[7] suggest incident response plans are made, but half of them are not tested. That means all kinds of unexpected events can and will delay response, leading to increased risk, damages and losses. Forensic readiness, or incident readiness, is a process often found lacking. In addition, audit logging and testing the plan periodically are regularly overlooked.

A second common issue we saw, especially for organisations with a lower cyber maturity, is **the patching itself**. Many organisations hadn't installed dependencies for the patch yet. Patching took hours or even days. Any delays caused by a more relaxed attitude to cyber hygiene have a negative business impact. Many are now making the case that for most businesses, managing on-premise solutions like Exchange doesn't make sense[8] anymore. While cloud solutions don't guarantee the absence of vulnerabilities, in this case, it certainly makes sense.

AN UNEXPECTED ISSUE: THE BLIND SPOT

This one might come as a surprise. Our last observation is about the second IR phase: *identification*. We found that many organisations don't have an 'as-complete-as-possible' inventory of digital assets. If you don't know what you have and where it is, finding the affected parts is impossible. Remember that many organisations acquire other companies, have different business owners with IT responsibilities, work in multiple countries with varying regulations, and work agile in biweekly deployment cycles. Even if you would find and contain 19 out of 20 exchange servers in time, you will still be breached. That is why having an asset inventory is vital. For reference, we consistently find 30-50% more organisational assets than were registered in their CMDB. A 30% blind spot is disastrous.

Over the last weeks, companies found two ways out of this:

1. Go searching under time pressure. Scanning netblocks, correlating email and DNS settings, asking experts... We found some organisations working the majority of the first weekend not on patching things but on finding things.
2. Make assumptions and accept risk. That option is not often chosen explicitly. We don't recommend this, even if it will free up your spare time.

HOW IS THIS GOING TO EVOLVE?

From our research into digital footprints and attack surfaces, we see steady growth and an increase in risk in attack surfaces. That means that in incident response, the *identify* phase will become even more important. In the future, the problem will shift further, from 'patch your stuff' to ‘find the stuff to patch’. For many mid-size organisations and larger, an attack surface technology will be essential.

Secondly, to deal with current threats and risk, you can’t solely rely on vulnerability management tools anymore. Intelligence is increasingly important to gather data and set priorities. For example, there are massive amounts of scans initiated looking for vulnerabilities. And you need a different kind of information when there is a PoC exploit released in the wild, or when active criminal or nation-state campaigns are being observed.

These factors are more important than any CVSS score when prioritising your patch efforts.

RECAP AND READINESS

Recapping all of this:

1. Zero days are here to stay and seem to occur more frequently.
2. Moving things to the cloud will not prevent everything, but it will offload some of the hygiene processes to a supplier.
3. Many organisations aren’t prepared (well enough) for these incidents. Two things often lacking are audit logging and periodical testing.
4. One lesser-documented issue is technology asset inventory. That means victims still need to find their affected infrastructure before they can patch it. In the incident response process, this means spending too much time in the *identify* phase.
5. We expect the focus to shift from ‘patching’ to ‘finding the stuff to patch’. For mid-sized organisations and above, an attack surface management technology is key to address these issues.

Incident response readiness is vital. Still, we identified gaps in many plans, causing many sysadmins to burn the midnight oil looking for their stuff rather than patching it. Response timelines are significantly reduced with a good attack surface inventory. It’s time to highlight this security and economic value, as your most recent vulnerabilities certainly won’t be the last ones you deal with this year.

SOURCES

1. https://techcommunity.microsoft.com/t5/exchange-team-blog/released-march-2021-exchange-server-security-updates/bc-p/2188142
2. https://www.cybersprint.com/news/microsoft-exchange-cve-how-to-scan-your-systems-for-the-vulnerability
3. https://msrc-blog.microsoft.com/2021/03/05/microsoft-exchange-server-vulnerabilities-mitigations-march-2021
4. https://www.darkreading.com/attacks-breaches/widely-known-flaw-in-pulse-secure-vpn-being-used-in-ransomware-attacks/d/d-id/1336729
5. https://badpackets.net/over-25000-citrix-netscaler-endpoints-vulnerable-to-cve-2019-19781/
6. https://www.bleepingcomputer.com/news/security/dearcry-ransomware-attacks-microsoft-exchange-with-proxylogon-exploits/
7. https://newsroom.ibm.com/2019-04-11-IBM-Study-More-Than-Half-of-Organizations-with-Cybersecurity-Incident-Response-Plans-Fail-to-Test-Them
8. https://www.crn.com/news/cloud/exchange-breach-msps-that-did-not-move-on-premise-exchange-to-the-cloud-blew-it-

ABOUT THE AUTHOR

EWARD DRIEHUIS has been a security veteran for over 24 years, describing himself as having a “tech heart, design mentality, and business drive”. He has a proven track record in innovative leadership in start-ups and largeenterprises. Eward is an established speaker in the media and at international events such as RSA and FS-ISAC,drawing upon his years of experience of fighting cyber threats together with banks, law enforcement and corporates.

Before joining Cybersprint, Eward spent three years as CMO at SecureLink, Europe’s largest cyber security provider, including being responsible for research. He has also spent nine years at Fox-IT heading their Threat Intelligence and Advanced Analytics products. Earlier in his career, Eward’s roles included CTO and Business Director in several IT and software companies.

ABOUT CYBERSPRINT

Cybersprint helps organisations achieve instant control over their visible and hidden digital risks to mitigate cyber threats related to their business, brand, online data and employees.

Our Our Attack Surface Management platform provides a continuous and automated process of identifying and managing your attack surface and associated external digital threats.

Visit www.cybersprint.com