GovCERT.HK

Weekly IT Security News Bulletin, 2021-W38

20 September – 26 September 2021

Headlines

Windows credentials leaked due to Microsoft's Autodiscover flaw

- Security researchers discovered an implementation issue in Microsoft's Autodiscover protocol that could expose users' Windows domain credentials. The Autodiscover protocol is a feature provided by Microsoft to simplify the configuration of new email accounts for applications such as Microsoft Outlook. With the Autodiscover feature, administrators or users can automatically configure a mail client by simply entering their domain credentials.

- After the domain credentials are provided, the Autodiscover process will try to access a list of URLs derived from the email address and fetch the related mail configuration until one of them succeeds. In case all of them fail, the process attempts to access pre-defined Autodiscover URLs in the same top-level domain that may belong to other organisations.

- If a threat actor controls these pre-defined domains or monitors their network traffic, the domain credentials being transmitted could be exposed. In addition, threat actors who control these domains can deceive mail clients to downgrade their authentication scheme from a secure protocol such as OAuth and NTLM to basic authentication.

Advice

- Set up web filtering firewalls to only whitelist legitimate or trusted Autodiscover domains and block all network traffic to other external Autodiscover domains.
- Disable basic authentication when deploying mail clients and consider disabling the Autodiscover feature.

Sources

- Guardicore
- Sophos
- BleepingComputer

Large-Scale phishing-as-a-service operation exposed

- Researchers uncovered a large-scale phishing-as-a-service (PHaaS) operation that offered phishing kits, email templates, hosting and automated services to carry out phishing attacks. The PHaaS service allowed threat actors to arrange phishing campaigns without specific technical capabilities and at a low cost.

- The operation has been active since 2018 and was used by multiple threat actors in either one-off or monthly subscription-based business models. Researchers estimated that it is responsible for many of the phishing campaigns that hit enterprises and organisations today. Offering over 100 phishing templates that mimic popular brands and services, it follows the legitimate software-as-a-service (SaaS) business subscription model for the development and distribution of tools to run phishing campaigns. The services also included tools for creating false sign-in pages, web hosting, and credential redistribution.

- One of the interesting aspects of this large-scale phishing campaign was that credentials stolen in phishing attacks by the customers of the service were also sent to a server controlled by PhaaS operators if they used a phishing kit in its default configuration. This double theft tactic allows the PhaaS operators to maximise their profits to resell victims' credentials.

Advice

- Be vigilant when clicking on any link or opening any attachments from unsolicited emails, even if they look official and legitimate.
- Adopt a security strategy to prevent, detect and respond to advanced phishing threats.
- Arrange user security awareness training regularly and include latest real-life phishing examples and phishing quizzes.

Sources

- Microsoft
- Security Affairs

Product Vulnerability Notes & Security Updates

1. Apple Products

https://support.apple.com/en-us/HT212816
https://support.apple.com/en-us/HT212818
https://support.apple.com/en-us/HT212825

2. Debian

https://www.debian.org/security/2021/dsa-4974
https://www.debian.org/security/2021/dsa-4975
https://www.debian.org/security/2021/dsa-4976
https://www.debian.org/security/2021/dsa-4977

3. F5 Products

https://support.f5.com/csp/article/K41997459

4. Huawei Products

https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20210922-01-commandinjection-en
https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20210922-01-ssrf-en
https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20210922-01-upload-en

5. IBM Products

https://www.ibm.com/support/pages/node/6490271
https://www.ibm.com/support/pages/node/6491795

6. McAfee

https://kc.mcafee.com/corporate/index?page=content&id=SB10367
https://kc.mcafee.com/corporate/index?page=content&id=SB10369

7. openSUSE

https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/5FC5F3EO3ROUN3SV32U3TNFWTKZ6B6TA/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/6ALRJGAG4EXTTIEI2CGMZH3NCUQIQUTQ/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/7GPSQYWLYZXIWWGB3O5ZPKMPADF4ZWBO/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/AFYTQFVWKBYVVXUN3DISYCDXS27AWFTC/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/ANLZ3MSWRYNRTSO7FPC7CORZ4WAS3YKE/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/AUF5M64CM26PNMNFO4R3S57DLRRNSTVG/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/FYZZYH2MI4PFNRWE2NZ5CTA5TOHKDLPC/

https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/GAT5MK7257FCSK4EI6CRDFI5ZVBUB5VC/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/JN7UM2F5HQYAKPOO75CIJNTXDGDU6ZTJ/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/UNTKFNNFNHHX5QOW7C4SZXLANXGXQCYJ/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/UQYGWX5BP3LA5ULPF6C7O7URBPXWRNFJ/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/W4HJ2XF2SFYPRBAICENTSEBE5KO7OY2G/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/WQJH6H27YAC2H2WM75ZCWCXIEK3AXNV3/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/XKFA6UOYGKCDBHHUW6MA56YT5KIDLCNF/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/YOWOZIQD7FWDNFL7CQF3WO5KZFKYYTDP/

8. Oracle Linux

https://linux.oracle.com/errata/ELSA-2021-3572.html
https://linux.oracle.com/errata/ELSA-2021-3576.html
https://linux.oracle.com/errata/ELSA-2021-3582.html
https://linux.oracle.com/errata/ELSA-2021-3585.html
https://linux.oracle.com/errata/ELSA-2021-3590.html
https://linux.oracle.com/errata/ELSA-2021-3623.html
https://linux.oracle.com/errata/ELSA-2021-9452.html
https://linux.oracle.com/errata/ELSA-2021-9453.html
https://linux.oracle.com/errata/ELSA-2021-9457.html
https://linux.oracle.com/errata/ELSA-2021-9458.html
https://linux.oracle.com/errata/ELSA-2021-9459.html
https://linux.oracle.com/errata/ELSA-2021-9460.html
https://linux.oracle.com/errata/ELSA-2021-9461.html

9. PHP

https://www.php.net/archive/2021.php#2021-09-23-1
https://www.php.net/archive/2021.php#2021-09-23-2
https://www.php.net/archive/2021.php#2021-09-23-3

10. Red Hat

https://access.redhat.com/errata/RHSA-2021:3559
https://access.redhat.com/errata/RHSA-2021:3572
https://access.redhat.com/errata/RHSA-2021:3576
https://access.redhat.com/errata/RHSA-2021:3582
https://access.redhat.com/errata/RHSA-2021:3585
https://access.redhat.com/errata/RHSA-2021:3590
https://access.redhat.com/errata/RHSA-2021:3598
https://access.redhat.com/errata/RHSA-2021:3623
https://access.redhat.com/errata/RHSA-2021:3638
https://access.redhat.com/errata/RHSA-2021:3639
https://access.redhat.com/errata/RHSA-2021:3653
https://access.redhat.com/errata/RHSA-2021:3656

https://access.redhat.com/errata/RHSA-2021:3658
https://access.redhat.com/errata/RHSA-2021:3660

11. Slackware

https://www.slackware.com/security/viewer.php?l=slackware-security&y=2021&m=slackware-security.419283
https://www.slackware.com/security/viewer.php?l=slackware-security&y=2021&m=slackware-security.470289

12. SonicWall Products

https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-0020
https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-0021
https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-0022
https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-0024

13. SUSE

https://www.suse.com/support/update/announcement/2021/suse-su-20212937-2/
https://www.suse.com/support/update/announcement/2021/suse-su-20212966-2/
https://www.suse.com/support/update/announcement/2021/suse-su-20213004-2/
https://www.suse.com/support/update/announcement/2021/suse-su-20213017-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20213018-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20213019-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20213020-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20213044-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20213049-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20213073-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20213117-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20213119-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20213120-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20213121-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20213123-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20213124-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20213125-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20213140-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20213141-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20213144-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20213151-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20213170-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20213174-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20213177-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20213178-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20213179-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20213180-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20213181-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20213184-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20213187-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20213191-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20213192-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20213193-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20213194-1/

https://www.suse.com/support/update/announcement/2021/suse-su-20213196-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20213201-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20213202-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20213205-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20213206-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20213207-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20213209-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20213210-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20213211-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20213212-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20213213-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20213214-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20213215-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20213217-1/
https://www.suse.com/support/update/announcement/2021/suse-su-202114800-1/
https://www.suse.com/support/update/announcement/2021/suse-su-202114801-1/
https://www.suse.com/support/update/announcement/2021/suse-su-202114802-1/
https://www.suse.com/support/update/announcement/2021/suse-su-202114807-1/

14. Trane Products

https://us-cert.cisa.gov/ics/advisories/icsa-21-266-01
https://us-cert.cisa.gov/ics/advisories/icsa-21-266-02

15. Ubuntu

https://ubuntu.com/security/notices/USN-5071-3
https://ubuntu.com/security/notices/USN-5073-2
https://ubuntu.com/security/notices/USN-5073-3
https://ubuntu.com/security/notices/USN-5079-3
https://ubuntu.com/security/notices/USN-5079-4
https://ubuntu.com/security/notices/USN-5084-1
https://ubuntu.com/security/notices/USN-5085-1
https://ubuntu.com/security/notices/USN-5086-1
https://ubuntu.com/security/notices/USN-5087-1
https://ubuntu.com/security/notices/USN-5088-1
https://ubuntu.com/security/notices/USN-5089-1
https://ubuntu.com/security/notices/USN-5089-2

Sources of product vulnerability information:

- Apple
- Debian
- F5 Products
- Huawei
- IBM
- McAfee
- openSUSE
- Oracle Linux
- PHP
- Red Hat
- Slackware
- SonicWall
- SUSE
- Ubuntu
- US-CERT

Contact:

cert@govcert.gov.hk