INTRODUCTION

Discovery and some stuff

BlueKeep or CVE-2019-0708 is a vulnerability patched by Microsoft in its May 2019 Patch Tuesday. The vulnerability was reported by the UK National Cyber Security Centre but we don't know when. It means the vulnerability passed the Equity Process. The Equity Process qualifies if a vulnerability must be kept by UK secret services or must be reported to the vendor) (https://www.gchq.gov.uk/information/equities-process).

Nota0: There is 2 scenario here:

- 0 : They've known the vuln since long time and used it against their targets (Maybe shared with allies too...)
- 1 : They discovered it and submited to Equity Process and the result was a report to Microsoft. If you think you were a possible target for them, maybe doing some archeology in your packets capture can give you some surprise ;)

Vulnerability

Microsoft Advisory

From the microsoft advisory, here is the description:

"A remote code execution vulnerability exists in Remote Desktop Services – formerly known as Terminal Services – when an unauthenticated attacker connects to the target system using RDP and sends specially crafted requests. This vulnerability is pre-authentication and requires no user interaction. An attacker who successfully exploited this vulnerability could execute arbitrary code on the target system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. To exploit this vulnerability, an attacker would need to send a specially crafted request to the target systems Remote Desktop Service via RDP."

It means the vulnerability can be triggerred remotely, leading to an exploitation of the Remote Desktop Services – formerly known as Terminal Services –, giving at the end of the exploitation, the possibilityto gain a Remote Command Execution as NT/SYSTEM also know as the high privilege possible under a Windows system.

Little introduction to RDP exchanges communications

The so much appreciated Remote Desktop Protocol (RDP) connection sequence:

```
(01) [Client] ---------X.224 Connection Request----------------> [Server]
(02) [Client] <--------X.224 Connection Request----------------- [Server]
(02*) *Here the transport can switch from unencrypted to TLS*
(03) [Client] ---------MCS Connect Initial and GCC Create------> [Server]
(04) [Client] <--------MCS Connect Response and GCC Response---- [Server]
(05) [Client] ---------MCS Erect Domain Request----------------> [Server]
(06) [Client] ---------MCS Attach User Request-----------------> [Server]
(07) [Client] <--------MCS Attach User Confirm------------------ [Server]
(08) [Client] ---------MCS Channel Join Request----------------> [Server]
(09) [Client] <--------MCS Channel Join Confirm----------------- [Server]
(10) [Client] ---------Security Exchange-----------------------> [Server]
(11) [Client] ---------Client Information----------------------> [Server]
(12) [Client] <--------License Error---------------------------- [Server]
(13) [Client] <--------Demand Active---------------------------- [Server]
(14) [Client] ---------Confirm Active--------------------------> [Server]
(15) [Client] ---------Synchronize-----------------------------> [Server]
(16) [Client] ---------Control - Cooperate---------------------> [Server]
(17) [Client] ---------Control - Request Control---------------> [Server]
(18) [Client] ---------Persistent Key List---------------------> [Server]
(19) [Client] ---------Font List-------------------------------> [Server]
(20) [Client] <--------Synchronize------------------------------ [Server]
(21) [Client] <--------Control - Cooperate---------------------- [Server]
(22) [Client] <--------Control - Granted Control---------------- [Server]
(23) [Client] <--------Font Map--------------------------------- [Server]
```

Schema reconstructed from Here

Some good read to better understanding the internals of RDP services and related

- ZeroDayInitiative: CVE-2019-0708: A COMPREHENSIVE ANALYSIS OF A REMOTE DESKTOP SERVICES VULNERABILITY
- McAfee: RDP Stands for “Really DO Patch!” – Understanding the Wormable RDP Vulnerability CVE-2019-0708
- Wazehell
- Medium: A debugging primer with CVE-2019-0708
- What happens before Hello?

The Blueteam side

Which are the vendors and versions impacted by the vulnerability?

Microsoft

Microsoft Windows impacted products list:

- Windows XP SP3 x86 Available Fix
- Windows XP Professionnel Édition x64 SP2 Available Fix
- Windows XP Embedded SP3 x86 Available Fix
- Windows Embedded POSReady 2009 Available Fix
- Windows Embedded Standard 2009 Available Fix
- Windows Server 2003 SP2 x86 Available Fix
- Windows Server 2003 Édition x64 SP2 Available Fix
- Windows Server 2003 R2 SP2 Available Fix
- Windows Server 2003 R2 Édition x64 SP2 Available Fix

- Windows Vista SP2 Available Fix
- Windows Vista Édition x64 SP2 Available Fix
- Windows 7 for 32-bit Systems Service Pack 1 Available Fix
- Windows 7 for x64-based Systems Service Pack 1 Available Fix
- Windows Server 2008 for 32-bit Systems Service Pack 2 Available Fix
- Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation) Available Fix
- Windows Server 2008 for Itanium-Based Systems Service Pack 2 Available Fix
- Windows Server 2008 for x64-based Systems Service Pack 2 Available Fix
- Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation) Available Fix
- Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1 Available Fix
- Windows Server 2008 R2 for x64-based Systems Service Pack 1 Available Fix
- Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) Available Fix

Sources:

- Microsoft Security Advisory
- Microsoft Customer Guidance for EoL Products

Siemens

Affected products, versions & Remediation

- SYSTEM ACOM.NET, Mat. Nr. 04815549: VC20A, VC21B, VC22B and VX22A; Disable Remote Desktop Protocol (RDP)
- System ACOM.net 2.0, Mat. Nr. 05568386: VC20A, VC21B, VC22B and VX22A; Disable Remote Desktop Protocol (RDP)

- System ACOM-Net, Mat. Nr. 5903872: VC20A, VC21B, VC22B and VX22A; Disable Remote Desktop Protocol (RDP)
- Sensis SIS Server Machine, Mat. Nr. 06648153: VC11C/D, VC12B/C, VC12L/M; Follow “Workarounds and Mitigations” until a patch is available
- Sensis High End SIS Server, Mat. Nr. 10140973: VC11C/D, VC12B/C, VC12L/M; Follow “Workarounds and Mitigations” until a patch is available
- SENSIS Dell High-End Server (VC12), Mat. Nr. 10910620: VC11C/D, VC12B/C, VC12L/M;Follow “Workarounds and Mitigations” until a patch is available
- VM SIS Virtual Server, Mat. Nr. 10765502: VC11C/D, VC12B/C, VC12L/M; Follow “Workarounds and Mitigations” until a patch is available
- AXIOM Multix M: All versions with Canon detector; Contact Siemens Regional Support Center.
- AXIOM Vertix MD Trauma: All versions with Canon detector; Contact Siemens Regional Support Center.
- AXIOM Vertix Solitaire M: All versions with Canon detector; Contact Siemens Regional Support Center.
- MOBILETT XP Digital: All versions with Canon detector; Contact Siemens Regional Support Center.
- MULTIX PRO ACSS P: All versions with Canon detector; Contact Siemens Regional Support Center.
- MULTIX PRO P: All versions with Canon detector; Contact Siemens Regional Support Center.
- MULTIX PRO/PRO ACSS/PRO Navy: All versions with Canon detector; Contact Siemens Regional Support Center.
- MULTIX Swing: All versions with Canon detector; Contact Siemens Regional Support Center.
- MULTIX TOP: All versions with Canon detector; Contact Siemens Regional Support Center.
- MULTIX TOP ACSS: All versions with Canon detector; Contact Siemens Regional Support Center.
- MULTIX TOP P/TOP ACSS P: All versions with Canon detector; Contact Siemens Regional Support Center.
- VERTIX SOLITAIRE: All versions with Canon detector; Contact Siemens Regional Support Center.
- Atellica Solution: All versions; Siemens Healthineers will provide additional updates regarding the plan and the details of activities required to increase the system security level.

- Aptio by Siemens: All versions; Siemens Healthineers will provide additional updates regarding the plan and the details of activities required to increase the system security level. -Aptio by Inpeco: All versions; Siemens Healthineers will provide additional updates regarding the plan and the details of activities required to increase the system security level.
- StreamLab: All versions; Siemens Healthineers will provide additional updates regarding the plan and the details of activities required to increase the system security level.
- CentraLink: All versions; Siemens Healthineers will provide additional updates regarding the plan and the details of activities required to increase the system security level.
- syngo Lab Process Manager: All versions; Siemens Healthineers will provide additional updates regarding the plan and the details of activities required to increase the system security level.
- Viva E: All versions;Siemens Healthineers will provide additional updates regarding the plan and the details of activities required to increase the system security level.
- Viva Twin: All versions;Siemens Healthineers will provide additional updates regarding the plan and the details of activities required to increase the system security level.
- Atellica COAG 360: All versions on Windows 7; No immediate action required. Patch will be available on 2019-06-03. Please see “workarounds and mitigations” for interim countermeasures.
- Atellica NEPH 630: All versions on Windows 7; No immediate action required. Patch will be available on 2019-06-03. Please see “workarounds and mitigations” for interim countermeasures.
- BCS XP: All versions on Windows 7; Patch will be available on 2019-06-03. Please see “workarounds and mitigations” for interim countermeasures.
- BCS XP: All versions on Windows XP; Patch will be available on 2019-06-03. Please see “workarounds and mitigations” for interim countermeasures.
- BN ProSpec: All versions on Windows 7; Patch will be available on 2019-06-03. Please see “workarounds and mitigations” for interim countermeasures.
- BN ProSpec: All versions on Windows XP; Patch will be available on 2019-06-03. Please see “workarounds and mitigations” for interim countermeasures.

- CS 2000 (supported by Sysmex - for information only): All versions on Windows 7; Patch availability under investigation. Please see “workarounds and mitigations” for interim countermeasures.
- CS 2000 (supported by Sysmex - for information only): All versions on Windows XP; Patch availability under investigation. Please see “workarounds and mitigations” for interim countermeasures.
- CS 2100 (supported by Sysmex - for information only): All versions on Windows 7; Patch availability under investigation. Please see “workarounds and mitigations” for interim countermeasures.
- CS 2100 (supported by Sysmex - for information only): All versions on Windows XP; Patch availability under investigation. Please see “workarounds and mitigations” for interim countermeasures.
- CS 2500 (supported by Sysmex - for information only): All versions on Windows 7; Patch availability under investigation. Please see “workarounds and mitigations” for interim countermeasures.
- CS 5100 (supported by Sysmex - for information only): All versions on Windows 7; Patch availability under investigation. Please see “workarounds and mitigations” for interim countermeasures.
- CS 5100 (supported by Sysmex - for information only): All versions on Windows XP; Patch availability under investigation. Please see “workarounds and mitigations” for interim countermeasures.
- AUWi: All versions; No immediate action required. Patch will be available in June 2019. Please see “workarounds and mitigations” for interim countermeasures.
- AUWi Pro: All versions; No immediate action required. Patch will be available in June 2019. Please see “workarounds and mitigations” for interim countermeasures.
- Rapid Point 500: Version 2.2; No immediate action required. Patch will be available in June 2019. Please see “workarounds and mitigations” for interim countermeasures.
- Rapid Point 500: Version 2.2.1; No immediate action required. Patch will be available in June 2019. Please see “workarounds and mitigations” for interim countermeasures.
- Rapid Point 500: Version 2.2.2; No immediate action required. Patch will be available in June 2019. Please see “workarounds and mitigations” for interim countermeasures.
- Rapid Point 500: Version 2.3; No immediate action required. Patch will be available in June 2019. Please see “workarounds and mitigations” for interim countermeasures.

- Rapid Point 500: Version 2.3.1; No immediate action required. Patch will be available in June 2019. Please see “workarounds and mitigations” for interim countermeasures.
- Rapid Point 500: Version 2.3.2; No immediate action required. Patch will be available in June 2019. Please see “workarounds and mitigations” for interim countermeasures.
- Lantis: All versions; Disable Remote Desktop Protocol (RDP) or close port 3389/tcp
- MagicLinkA: All versions; Apply all the appropriate security patches released by Microsoft. Installation of Windows patches and hotfixes is the responsibility of product operator, unless otherwise agreed. The compatibility of Microsoft security patches with products from Siemens Healthineers that are beyond their End of Support date cannot be guaranteed.
- MagicView1000W: All versions; Apply all the appropriate security patches released by Microsoft. Installation of Windows patches and hotfixes is the responsibility of product operator, unless otherwise agreed. The compatibility of Microsoft security patches with products from Siemens Healthineers that are beyond their End of Support date cannot be guaranteed.
- MagicView300: All versions; Apply all the appropriate security patches released by Microsoft. Installation of Windows patches and hotfixes is the responsibility of product operator, unless otherwise agreed. The compatibility of Microsoft security patches with products from Siemens Healthineers that are beyond their End of Support date cannot be guaranteed.
- Medicalis Clinical Decision Support: All versions; Apply all the appropriate security patches released by Microsoft. Installation of Windows patches and hotfixes is the responsibility of product operator, unless otherwise agreed. The compatibility of Microsoft security patches with products from Siemens Healthineers that are beyond their End of Support date cannot be guaranteed.
- Medicalis Intelligo: All versions; Apply all the appropriate security patches released by Microsoft. Installation of Windows patches and hotfixes is the responsibility of product operator, unless otherwise agreed. The compatibility of Microsoft security patches with products from Siemens Healthineers that are beyond their End of Support date cannot be guaranteed.

- Medicalis Referral Management: All versions; Apply all the appropriate security patches released by Microsoft. Installation of Windows patches and hotfixes is the responsibility of product operator, unless otherwise agreed. The compatibility of Microsoft security patches with products from Siemens Healthineers that are beyond their End of Support date cannot be guaranteed.
- Medicalis Workflow Orchestrator: All versions; Apply all the appropriate security patches released by Microsoft. Installation of Windows patches and hotfixes is the responsibility of product operator, unless otherwise agreed. The compatibility of Microsoft security patches with products from Siemens Healthineers that are beyond their End of Support date cannot be guaranteed.
- Screening Navigator: All versions; Apply all the appropriate security patches released by Microsoft. Installation of Windows patches and hotfixes is the responsibility of product operator, unless otherwise agreed. The compatibility of Microsoft security patches with products from Siemens Healthineers that are beyond their End of Support date cannot be guaranteed.
- syngo Dynamics: VA10 and earlier; Apply all the appropriate security patches released by Microsoft. Installation of Windows patches and hotfixes is the responsibility of product operator, unless otherwise agreed. The compatibility of Microsoft security patches with products from Siemens Healthineers that are beyond their End of Support date cannot be guaranteed.
- syngo Imaging: All versions; Apply all the appropriate security patches released by Microsoft. Installation of Windows patches and hotfixes is the responsibility of product operator, unless otherwise agreed. The compatibility of Microsoft security patches with products from Siemens Healthineers that are beyond their End of Support date cannot be guaranteed.
- syngo Plaza: All versions; Apply all the appropriate security patches released by Microsoft. Installation of Windows patches and hotfixes is the responsibility of product operator, unless otherwise agreed. The compatibility of Microsoft security patches with products from Siemens Healthineers that are beyond their End of Support date cannot be guaranteed.
- syngo Workflow MLR: All versions; Apply all the appropriate security patches released by Microsoft. Installation of Windows patches and hotfixes is the responsibility of product operator, unless otherwise agreed. The

compatibility of Microsoft security patches with products from Siemens Healthineers that are beyond their End of Support date cannot be guaranteed.

- syngo Workflow SLR: All versions; Apply all the appropriate security patches released by Microsoft. Installation of Windows patches and hotfixes is the responsibility of product operator, unless otherwise agreed. The compatibility of Microsoft security patches with products from Siemens Healthineers that are beyond their End of Support date cannot be guaranteed.
- syngo.via: All versions; Apply all the appropriate security patches released by Microsoft. Installation of Windows patches and hotfixes is the responsibility of product operator, unless otherwise agreed. The compatibility of Microsoft security patches with products from Siemens Healthineers that are beyond their End of Support date cannot be guaranteed.
- syngo.via View&GO: All versions; Apply all the appropriate security patches released by Microsoft. Installation of Windows patches and hotfixes is the responsibility of product operator, unless otherwise agreed. The compatibility of Microsoft security patches with products from Siemens Healthineers that are beyond their End of Support date cannot be guaranteed.
- syngo.via WebViewer: All versions; Apply all the appropriate security patches released by Microsoft. Installation of Windows patches and hotfixes is the responsibility of product operator, unless otherwise agreed. The compatibility of Microsoft security patches with products from Siemens Healthineers that are beyond their End of Support date cannot be guaranteed.
- teamplay (receiver software only): All versions; Apply all the appropriate security patches released by Microsoft. Installation of Windows patches and hotfixes is the responsibility of product operator, unless otherwise agreed. The compatibility of Microsoft security patches with products from Siemens Healthineers that are beyond their End of Support date cannot be guaranteed.

Sources:

- Siemens Security Advisory
- Siemens Security Advisory

- Siemens Security Advisory
- Siemens Security Advisory
- Siemens Security Advisory
- Siemens Security Advisory

Huawei

Affected Product name and version

- SMC2.0 Version(s): V500R002C00 & V600R006C00, Follow the Microsoft security advisory to implement patch or workaround

source: https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20190529-01-windows-en

Countermeasures

Enable Network Level Authentication [NLA]

Why ?

If you enable NLA, in the RDP exchange schema, attackers are stopped at step 1.

Supported Versions

On the server side:

- Windows 2008
- Windows 2008 R2
- Windows 7

- Windows Vista

On the client side:

- Windows XP SP3
- Windows Vista
- Windows 7
- Windows 2008
- Windows 2008 R2
- Remote Desktop Connection for Mac

How ?

- Server GPO

```
Computer Configuration
  Policies
    Administrative Templates
      Windows Components
        Remote Desktop Settings
          Remote Desktop Session Host
            Security
              Require user authentication for remote connections by using Network Level Authenticat
               Enabled
                OK
```

- Client GPO

```
Computer Configuration
  Policies
    Administrative Templates
      Windows Components
        Remote Desktop Settings
          Remote Desktop Connection Client
            Configure Authentication for Client
              Enabled
                OK
```

SwiftOnSecurity Recommendations

Swift On Security

Block 3389 trafic from the internet

I know, some people can't. Author's note: some specific configurations set the RDP to listen on another port number. Adapt your signatures and detections in consequences.

Disable RDP services on your machines

If you don't used it, disable it.

How to detect it?

Network signatures

NCC group released a network signature using Suricata: https://github.com/nccgroup/Cyber-Defence/blob/b2965daaa7bd89779bee95ad6b8c1bfed3821fda/Signatures/suricata/2019_05_rdp_cve_2019_0708.t xt

EmergingThreats Labs released a network signature supporting Suricata and Snort:

- Suricata
- Snort

Author's note: some specific configurations set the RDP to listen on another port number. Adapt your signatures and detections in consequences.

Network signatures detections limits

If the attacker requests a TLS connection, current network signatures aren't more relevant, because the trafic is encrypted. Except if you have the ability to configure TLS interception on your sensors. Talos Security published a guide to do it for Firepower sensors but i'm pretty sure it's supported by others vendors: https://blog.talosintelligence.com/2019/05/firepower-encrypted-rdp-detection.html

The magic cookie name (zerosum0x0 default scanner)

As explained by @bromiley, @zerosum0x0 set up a cookie name in his scanner. This specific Cookie value is five random characters and has a protocol request of 0x00000000. Easy to spot with a network sig.

source: https://medium.com/@bromiley/what-happens-before-hello-ce9f29fa0cef

The account name (zerosum0x0 default scanner)

As explained by @AdamTheAnalyst, @zerosum0x0 used for his scanner by default an interesting user account name "AAAAAAA" when someone use the default metasploit scan module against your device. You can find this information in your logs under the Event ID 4625 (you need to have activated the logging, even for the missed authentification ones) As people can change a little bit the default scanner values and if you have a strict user account name policy, you can create your own regex for this part based on your policy.

source: https://twitter.com/adamtheanalyst/status/1134394070045003776?s=21

Security Solutions Detections

Symantec

- 31527 OS Attack: Microsoft Windows Desktop Services RCE CVE-2019-0708
- 31529 OS Attack: Microsoft Windows Desktop Services RCE CVE-2019-0708 2

McAfee

0x47900c00 RDP: Microsoft Remote Desktop MS_T120 Channel Bind Attempt

Kaspersky

I'm confident Exploit Prevention (EP) is able to detect the attack, but I have no proof.

Fsecure

No public detection, you can scan your environment, use the plugin 1013880 for it.

Checkpoint

The protection is available in SandBlast Agent’s E80.97 Client Version (Can be downloaded from sk154432).

EXPLOITATION

Exploits type:

- DoS (Publicly available)
- RCE (Publicly available)
- LPE (Privately available)

TIMELINE (AFAIK)

- N/A @NCSC privately report the vulnerability to @msftsecurity
- 2019-05-14 @msftsecurity published the vulnerability advisory
- 2019-05-14 @msftsecresponse Chief blogpost about it
- 2019-05-15 00:47 The name of the vulnerability will be BlueKeep, reference to the Red Keep in Game of Thrones and cause often exploit like this cause Blue Screen of Death
- 2019-05-15 10:25 @cBekrar confirmation (RCE)
- 2019-05-16 19:28 (Un)Oficial logo was released by @GossiTheDog
- 2019-05-17 20:05 @ValthekOn confirmed (no info)
- 2019-05-17 22:19 @ChristiaanBeek confirmed the @ValthekOn PoC
- 2019-05-20 10:20 360Vulcan team made a vulnerability scanner and you must ask them by mail to know your vulnerable status
- 2019-05-20 11:04 @oct0xor confirmation (BSoD)
- 2019-05-21 00:45 @TalosSecurity release snort sig
- 2019-05-21 @McAfee_Labs published details about it (RCE)
- 2019-05-21 10:46 @*CPResearch* confirmation (BSoD)
- 2019-05-21 11:03 @NCCGroupInfosec released suricata sig

- 2019-05-22 @RandoriSecurity confirmation (BSoD
- 2019-05-22 02:48 @zerosum0x0 & @JaGoTu released a public scanner
- 2019-05-22 11:59 360Vulcan Team released their scanner after someone uploaded it on Virus Total
- 2019-05-22 17:33 @RedDrip7 confirmation (BSoD)
- 2019-05-23 12:42 @mj0011sec confirmation (RCE)
- 2019-05-24 06:41 @malwaretechblog has a working PoC (BSoD)
- 2019-05-24 17:3e @0patch release a patch who's not need to reboot the machine after (PRO version, not Free)
- 2019-05-25 03:49 @GreyNoiseIO said there is a wide scan from Tor seeking
- 2019-05-30 MIcrosoft Security Chief Pope published a second warning blogpost about the threat
- 2019-05-30 17:37 @n1xbyte DoS exploit published (publicly)
- 2019-05-30 17:57 @ret2got published Perfect.blue team DoS exploit (publicly)
- 2019-05-30 Exploit-DB published the @n1xbyte exploit
- 2019-05-31 11:27 @ChristiaanBeek said there's an offer for a weaponized PoC (50K)
- 2019-06-01 10:00 @zerosum0x0 had a full RCE
- 2019-06-02 02:17 @ryHanson said he had a full RCE
- 2019-06-04 13:12 @zerosum0x0 & @Jagotu has a private Metasploit module for RCE
- 2019-06-07 07:05 @theori_io claim had an RCE
- 2019-07-05 21:08 @ksecurity45 claimed had an RCE (video showed an unstable one)
- 2019-07-19 Mr. Yang Jiewei, senior researcher at TENCENT KeenLab gave a presentation of the vulnerability and released the slides of the conference publicly
- 2019-07-22 19:24 @SpecialHoang and @nixbyte claim they had an LPE version of BlueKeep
- 2019-07-23 11:30 @0xeb_bp released a detailed write-up containing lot of useful information

- 2019-07-23 21:43 @Immunityinc claimed to selling RCE version of BlueKeep commercially inside their CANVAS 7.23
- 2019-09-06 18:35 @metasploit released the RCE (limited to some version and need manual information on the target)
- 2019-09-06 20:12 @zerosum0x0 released his own RCE PoC with less restrictions but more unstable