

**27/11/2024**

**CP Plus**

# **Security Assessment Report**

**CP-VNR-3104 NVR**

**Firmware version B3223P22C02424**

# Company Details

Company Name	CPPLus - Aditya Infotech Ltd.(CP PLUS)
Email	support@cpplusworld.com
Telephone	+91-8800952952

# Document History

Version	Date	Author	Remark
1.0	27/11/2024	Yashodhan Vivek Mandke	First Draft

# Security Assessment Details

## 1.1 Executive Summary

Security Assessment of **CP-VNR-3104 NVR Firmware version B3223P22C02424** model has been performed, considering below common security issues:

- ✓ If firmware has any vulnerabilities

Overall security postures of the device are good, though some of the security controls/measures have not been properly thought of/implemented during the design and coding of the application.

The security assessment revealed 5 High severity issue in this product.

The consolidated summary of the assessment has been presented in the Executive Summary section. Additional information is contained within the Detailed Vulnerability Information section of this report.

## 1.2 Scope and Objectives

The scope of this assessment was limited to Firmware of **CP-VNR-3104** NVR.

## 1.3 Technology Impact Summary

The security assessments on the Firmware has been performed. These assessments aim is to uncover any security issues in the assessed NVR to explain the impact and risks associated with the found issues, and provide guidance in the prioritization and remediation steps.

It was identified that firmware has private keys and certificates extracted from it.

## 1.4 Testing Environment and Tools

To perform hardware security assessment over the **CP-VNR-3104 NVR Firmware version B3223P22C02424** tools such as Binwalk and GNU Strings

## 1.6 Table of Findings

Vulnerability ID	Scope	Finding	CVSS Score	CVSS String	Severity	Reserved CVE
CP-NVR-01	Firmware	First static RSA Key extracted	<a href="#">8.5</a>	CVSS:4.0/ AV:L/ AC:L/ AT:N/ PR:N/ UI:N/ VC:H/ VI:N/ VA:N/ SC:H/SI:H/ SA:H	High	CVE-2024-54849
CP-NVR-02	Firmware	EC Key extracted	<a href="#">8.5</a>	CVSS:4.0/ AV:L/ AC:L/ AT:N/ PR:N/ UI:N/ VC:H/ VI:N/ VA:N/ SC:H/SI:H/ SA:H	High	CVE-2024-54846
CP-NVR-03	Firmware	Second static RSA Key extracted	<a href="#">8.5</a>	CVSS:4.0/ AV:L/ AC:L/ AT:N/ PR:N/ UI:N/ VC:H/ VI:N/ VA:N/ SC:H/SI:H/ SA:H	High	Duplicate of CVE-2024-54849
CP-NVR-04	Firmware	Certificate	<a href="#">8.5</a>	CVSS:4.0/	High	CVE-2024-

		extracted		AV:L/ AC:L/ AT:N/ PR:N/ UI:N/ VC:H/ VI:N/ VA:N/ SC:H/SI:H/ SA:H		54848.
CP-NVR-05	Firmware	Static DH Parameters in Firmware	<a href="#">8.5</a>	CVSS:4.0/ AV:L/ AC:L/ AT:N/ PR:N/ UI:N/ VC:H/ VI:N/ VA:N/ SC:H/SI:H/ SA:H	High	CVE-2024- 54847.

# Technical Findings

## 2.1 CP-NVR-01: First static RSA Key extracted ( Reserved CVE : CVE-2024-54849)

Potential Impact : **High**

### Description :

During the assessment it was identified that the RSA private key was hardcoded available in firmware

**Affected Hosts** : Device firmware, device identity, authentication.

### Steps to Reproduce:

- 1 Download firmware from CP Plus website and select the product to be pen tested.

The screenshot shows the CP Plus website's firmware download page. The browser address bar displays 'cpplusworld.com/firmware'. The website header includes the CP Plus logo and navigation links: Home, Products, Marketing, Solutions, Support, Training, and Contact Us. A search icon is also present.

On the left sidebar, there is a 'Filter By' section with a 'Product' dropdown and a search box labeled 'Enter Model No.'. Below this is a 'FILTER' button. The 'Categories' section lists 'Download (04)', 'Tools (02)', 'Others (04)', and 'Support'. At the bottom of the sidebar are three contact options: 'Call Us' with the number 8800952952, 'Write Us' with a link to write support, and 'Live chat'.

The main content area displays two sections of firmware downloads. The first section is titled 'Orange' and shows 'We found 11 Items'. It contains a table with the following data:

Model No.	Version	Uploaded On	Release Note	Download
CP-UVR-0808K1-H	V4.000.00AT008.0	Mar, 01 2023		
CP-UVR-1601E1-H	V4.000.00AT008.0	Mar, 01 2023		
CP-UVR-0801K1-H	V4.000.00AT008.0	Mar, 01 2023		
CP-UVR-1601E2-H	V4.000.00AT008.0	Mar, 01 2023		
CP-UVR-0401L1B-4KH	V4.000.00AT008.0	Mar, 01 2023		
CP-UVR-0401L1-4KH	V4.000.00AT008.0	Mar, 01 2023		
CP-UVR-1601E1-HC	V4.000.00AT008.0	Mar, 01 2023		
CP-UVR-0801F1-HC	V4.000.00AT008.0	Mar, 01 2023		

The second section is titled 'Indigo' and shows 'SHOW ALL'. It contains a table with the following data:

Model No.	Version	Uploaded On	Release Note	Download
CP-VNR-3104	B3223P22C02424	Jul, 15 2023		
CP-VNR-3108	B3223P22C02424	Jul, 15 2023		
CP-VNR-3208	B3223P22C02424	Jul, 15 2023		

**CP-VNR-3104**

4 Ch. 4K Network Video Recorder

- 4 Channel IP Camera Input
- Ultra 265/H.265/H.264 dual Video Formats
- Support 4K Resolution Upto 8MP Recording
- 40Mbps Incoming/ 48Mbps Outgoing Bandwidth
- Support 1 SATA HDDs up to 10TB, 2 USB Ports
- Support Multi-brand network cameras
- Mobile Software: Android, IOS
- CMS Software: IVMS
- \*Only for UAE

[Datasheet](#)**Specification****Request for Information**

Processor	Dual-core embedded processor
Operating System	Embedded LINUX
Bandwidth Incoming	40Mbps
User Interface	GUI



## 2 Downloaded firmware



## 3 Extract the firmware binary using binwalk

```

ments/nvr_cp_plus/firmware$ binwalk -e b997748b-ec6d-4d45-9098-78c435982ccc.
bin

```

DECIMAL	HEXADECIMAL	DESCRIPTION
486984	0x76E48	CRC32 polynomial table, little endian
494637	0x78C2D	Sega MegaDrive/Genesis raw ROM dump, Name: "", "K
50268	0x83E6C	Android bootimg, kernel size: 1866861056 bytes, k
577680	0x8D090	gzip compressed data, has original file name: "bo
588980	0x8FCB4	uImage header, header size: 64 bytes, header CRC:
589044	0x8FCF4	Linux kernel ARM boot executable zImage (little-e

#### 4 Navigate to the directory and start analyzing the extracted file system

```

essments/nvr_cp_plus/firmware/_b997748b-ec6d-4d45-9098-78c435982ccc.bin.extract
ed$ ls
14A5F86      14A7912.xz  14AA33C      14AD308.xz  1514214.gz
14A5F86.xz  14A8044      14AA33C.xz  14AE506      16138DA.tar
14A6748      14A8044.xz  14AADC2      14AE506.xz  33EF74.yaffs
14A6748.xz  14A878E      14AADC2.xz  14AEB18      342034.squashfs
14A6D12      14A878E.xz  14AB818      14AEB18.xz  928CC
14A6D12.xz  14A8F18      14AB818.xz  14AED0E      928CC.7z
14A7298      14A8F18.xz  14AC332      14AED0E.xz  bootlogo_zh.jpg
14A7298.xz  14A94FA      14AC332.xz  14AF50C      squashfs-root
14A7912      14A94FA.xz  14AD308      14AF50C.xz

```

#### 5 Extract 33EF74.yaffs from binwalk and run strings on the internal file

```

stellaris@stellaris-VivoBook-ASUSLaptop-X513EAN-K513EA:~/Documents/Security_assessm
ents/nvr_cp_plus/_b997748b-ec6d-4d45-9098-78c435982ccc.bin.extracted/_33EF74.yaffs.
extracted/_1168324.xz.extracted$ strings 67A.xz

```



6 In the strings output one of the finding is RSA private key

```
-----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAAKCAQEAyHTEzLn5tXnpRdkUYLB9u5Pyax6fM60Nj4o8VmXl3ETZzGaF
B9X4J7BKNdBjngpuG7fa8H6r7gwQk4ZJGDTzqCrSV/Uu1C93KYRhTYJQj6eVSHD1
bk2y1RPD0hrt5kPqQhTrd0rA7R/UV06p86jt0uDBMHEwMjDV0/YI0FZPRo7yX/k9
Z5GIMC5Cst99++UMd//sMcB4j7/Cf8qtbCHWjdmLao5v4Jv4EFbMs44TFeY0BGbH
7vk2DmqV9gmaBmf0ZXH4yqSxJeD+PIs1BGe64E92hfx//DZrtenNLQNiTrM9AM+v
dqBpVoNq0qjU51Bx5rU2BXcFbXvI5MT9TNUhXwIDAQABAoIBAGdNtfYDiap6bzst
yhCiI8m9TtrhZw4MisaEaN/ll3XSjaOG2dvV6xMZCMV+5TeXDH0AZnY18Yi18vzz
4Ut2TnNFzizCECYNaA2fST3WgInnxUkV3YXAYP6CNxJaCmv2aA0yFr2kFVSeaKGt
ymvljNp2NVkvm7Th8fBQB07I7AXhz43k0mR7XmPgewe8ApZ0G3hstkoAmvbWAvWA
zCZupdDjZYj0JqlA4eEA4H8/w7F83r5CugeBE8LgEREjLPiyejrU5H1fubEY+h0d
l5HZBJ68ybTXfQ5U9o/QKA3dd0toBEhhdRUDGzWtjvwkEQfqF1reGWj/tod/gCpf
DFi6X0ECgYEA4w0v/pjSC3ty6Tu0vKX2r0UiBrLXXv2JSxZnMoMiWI5ipLQt+RYT
VPafL/m7Dn6Mbwjay0kcZhBwk5CNz5A6Q4lJ64Mq/lqHznRCQQ2Mc1G8eyDF/fYL
Ze2pLvwP9VD5jTc2miDfw+MnvJhywRRLcemDFP8k4hQVtm8PMp3ZmNECgYEA4gz7
wz0bR4gn8ibe617uQPZjWzUj9dUHYd+inlgwBCIrtNnaRn9I9U/Q6tegRYpii4ys
c176NmU+umy6XmuSKV5qD9bSpZWG2nLFnslnN15Lm3fhZxoeMNHBaEDTnLT26yoi
33gp0mSSWy94ZEqipms+ULF6sY1ZtFW6tpGFoy8CgYAQHhnnvJfLIIs2ky4q10B60
ZcxFp3rtDpkp0JxhFLhiizFrujMtZSjYNm5U7KkgPVHhLELEUvCm0nKTt4ap/vZ0
BxJNe1GZH3pW6SAvGDQpl9sG7uu/vTFP+lCxukmzxB0DrrDcvorEkKMom7ZCCrvW
KZsZ6YeH2Z81BauRj218kQKBgQCUV/DgKP2985xDTT79N08jUo3hTP5MVYCCuj/+
UeEw1TvZcx3LJby7P6Xad6a1/BqveaGyFKIfEFiABUBItk801sDDpDaYc4gL00Xc
7lFuBH0ZkxJYlss5QrGpu0El9ZwUt5IrFLBdYaKqNHzNVC1pCPfb/JyH6Dr2HUxq
gxUwAQKBgQCcU6G2L8AG9d9c0Up0yL1tMvFe5Ttw0KjLQVdsh1MP6yigYo9DYuwu
bHFVW2r0dBTqegP2/KT0xKzaHfC1qf0RGDsUoJCNJrd1cwoCLG8P2EF4w30BrKqv
8u4ytY0F+Vlanj5lm3TaoHSVF1+NWPY0TiwevIECGKwSxviki4fDAA==
-----END RSA PRIVATE KEY-----
```

## 2.2 CP-NVR-02: EC Key extracted (Reserved CVE : CVE-2024-54846)

Potential Impact : **High**

### **Description :**

During the assessment it was identified that the EC private key was hard coded available in firmware

**Affected Hosts** : Device firmware, device identity, authentication.

Steps to Reproduce:

- 1 Continue analyzing same file extracted by gnu strings
- 2 EC private key is available in same file. There are 2 keys of EC.

```
-----BEGIN EC PRIVATE KEY-----
MHcCAQEEIPEqEyB2AnCoPL/9U/YDHvdqXYbIogTywwyp6/UfDw6noAoGCCqGSM49
AwEHoUQDQgAEN8xW2XYJHlpyPsdZLf8gbu58+QaRdNCtFLX3aCJZYpJ05QDYIxH/
6i/SNF1dFr2KiMJrdw1VzYoqDvoByLTt/w==
-----END EC PRIVATE KEY-----
```

```
-----BEGIN EC PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: DES-EDE3-CBC,307EAB469933D64E
IxbrRmKcAzctJqPdTQLA4SWyBYYGYJVkYEna+F7Pa5t5Yg/gKADrFKcm6B72e7DG
ihExtZI648s0zdYw6qSJ74vrPSuWDe5qm93Bqs fVH9svtCzWHW0pm1p0KTBCFfUq
UsuWTITwJImcnlAslgaRZ3sAWm7c0UIdL0fo2G0fYUFNcYoCSLffCFTEHBuPnagb
a77x/sY1Bvii8S9/XhDTb6pTMx06wzrm
-----END EC PRIVATE KEY-----
RelaySSLTest
```

## 2.3 CP-NVR-03: Second static RSA Key extracted (Reserved CVE : **Duplicate of** CVE-2024-54849)

Potential Impact : **High**

### **Description :**

During the assessment it was identified that the second RSA private key was hard coded available in firmware

**Affected Hosts :** Device firmware, device identity, authentication.

Steps to Reproduce:

- 1 Continue analyzing same file extracted by gnu strings.
- 2 Second RSA private key is available in same file.



```
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: DES-EDE3-CBC,A8A95B05D5B7206B
0Qd9GeArejl1GDVh2lLV1bHt0cPtfbh5h/5zVpAVaFpqtSPMrElp50Rntn9et+JA
7V0yboR+Iy2t/HU4WvA687k3Bppe9GwKHjHhtl//8xFKwZr3Xb5y05JUP8AUctQq
Nb8CLlZyuUC+52REAAthdWgsX+7dJ04yabzUcQ22Tp9JSD0hiL43BlkWYUNK3dAo
PZlmiptjnzVTjg1MxsBSydZinWOLBV8/JQgxSPo2yD4uEfig28qbvQ2wNIn0pnAb
GxnSA0azkongEGfvcjIIs+LZN9gXFhxc0h6kc4Q/c99B7QWETwLLkYgZ+z1a9VY9
gEU7CwCxYCD+h9hY6FPmsK0/lC407aeRKpYq00rPPxs6i7phiexg6ax6yTMmArQq
QmK3TAsJm8V/J5AwPLEV6jAFgRGymGGHnof0DXzVWZidrcZJWTNuGEX90nB3ee2w
PXJEFWKoD3K3aFcSLdHYr3mLGxP7H9ThQai9VsycxZKS5kwvBKQ//YMrMFfwPk8x
vTeY4KZMaUrveEel5tWZC94RSMKgXR6cyElNBXyTQnD0GbfpNNGBKxyKbINWo0JU
WJZAwlsQn+QzCDwpri7+sV1mS3gBE6UY7aQmnmiaC2V3Hbphxct/en5QsfD0t1X
JczSfpRWLlbPznZg80Qh/VgCMA58N5Dj0zTIK7sJJ5r+94ZBTCpgAMbF588f0NTR
KCe4yrxGJR7X02M4nvD4Iw0lpsQ8xQxZt0SgXv4LkxvdU9XJJKWZ/XNKJewztxSe
Z1vdTc2YfsDBA2SEv33vxHx2g1vqtw8SjDRT2RaQSS0QuSaMJimd0X6mTOCBKk1J
0Q5mXTrER+/LnK0jEmXsBXWA5bqqVZIyahXSx4VYZ7l7w/PHiUDtDgyRhMMKi4n2
lQvQcWSQTjrpnlJbca1/DkpRt3YwrvJwdqb8asZU2VrNETH5x0QVefDRLFiVpif/
tUaeAe/P1F80kS70IZDs1Subv/sD2vMbhnkUoCms3/PvNtdnvgL4F0zhaDpKCmlT
P8vx49E7v5CyRNmED9zZg4o3wmMqrQ093PtTug3Eu9oVx1zPQM1NVMyBa2+f29DL
lnuTCeXdo9+ni45xx+jAI4DCwrRdhJ9uzZyC6962H37H6D+5naNvClFR1s6li1Gb
nqPoiy/0BsEx9CaDGcQQBp5Wme/3XW+6z1ISOx+igwNTVCT14mHdBMbya0eIKft5
K+GnwtgEMyCYyyWuUct8g4RzErcY9+yW90m5Hzpx4z0uW4NPZgPDTgK+t2RSL/Yq
rE1njrgeGYcVeG3f+0ftH4s6fPbq7t1A5ZgUscbLMBqr9tK+0qygR4EgKBPsH6Cz
L6zlv/2RV0qAHvVuDJcIDIgwY5rJtINEm32rh0eFNJwZS5MNIC1czXZx5//ugX7l
I4sy5nbVhwSjtAk8Xg5dZbdTZ6mIrb7xqH+fdakZor1khG7bC2uIwibD3cSl2XkR
vN48ls1bHnqqagr6Xm1nN0SVl8C/6kbJEsMpLhAezfRtGwv0ucoaE+WbeUNolGde
P/eQiddSf0brnpiLJRh7qZrl9XuqYdpUqnoEdMAfotD0ID80tV7gt8a48ad8VPW2
-----END RSA PRIVATE KEY-----
```

## 2.4 CP-NVR-04: Certificates extracted (Reserved for :cve-2024-54848)

Potential Impact : **High**

### Description :

During the assessment it was identified that the certificates were available in firmware

**Affected Hosts** : Device firmware, device identity, authentication.

Steps to Reproduce:

- 1 Continue analyzing same file extracted by gnu strings.
- 2 Multiple certificates are available in same file.

```
CCM-AES #%u:
-----BEGIN CERTIFICATE-----
MIICUjCCAdegAwIBAgIJAMFD4n5iQ8zoMAoGCCqGSM49BAMCMD4xCzAJBgNVBAYT
Ak5MMREwDwYDVQQKEwhQb2xhc1NTTDEcMBoGA1UEAxMTUG9sYXJzc2wgVGVzdCBF
QyBDQTAeFw0xMzA5MjQxNTQ5NDhaFw0yMzA5MjQxNTQ5NDhaMD4xCzAJBgNVBAYT
Ak5MMREwDwYDVQQKEwhQb2xhc1NTTDEcMBoGA1UEAxMTUG9sYXJzc2wgVGVzdCBF
QyBDQTB2MBAGByqGSM49AgEGBSuBBAAiA2IABMPaKzRBN1gvlb+/Im6KUNLTuBu
ww5XUzM5WNRStJGV0Qsj318XJGJI/BqVKc4sLYfCiFKAr9ZqqyHduNMcbli4yuiy
aY7zQa0pw7RfdadHb9UZKVVpmLM7ILRmFmAzhQ0BoDCBnTAdBgNVHQ4EFgQUnW0g
JEkBPYvLeLUZvH4kydv7NnwWbgYDVR0jBGcwZYAUnW0gJEkBPYvLeLUZvH4kydv7
NnyhQqRAMD4xCzAJBgNVBAYTAk5MMREwDwYDVQQKEwhQb2xhc1NTTDEcMBoGA1UE
AxMTUG9sYXJzc2wgVGVzdCBFQyBDQYIJAMFD4n5iQ8zoMAwGA1UdEwQFMAMBAf8w
CgYIKoZIZj0EAWIDAQAuZGIXAM00YnNWKJUAfXgSJtJxexn4ipg+kv4znuR50v56
t4d0PCu412mUC6Nnd7izvtE2MgIXAP1nnJQjZ8BWukszFQDG48wxCCyci9qpdSMv
uCjn8pwU0kABXK8Mss90fzCfCE0tIA==
-----END CERTIFICATE-----
```

-----BEGIN CERTIFICATE-----

MIIDhzCCAm+gAwIBAgIBADANBgkqhkiG9w0BAQUFADA7MQswCQYDVQQGEwJ0TDER  
MA8GA1UEChMIUG9sYXJ0TU0wGTAxBgNVBAMTEFBvbGFyU1NMIFRlc3QgQ0EwHhcN  
MTUwMjE5MTQ0NDAwWhcNMjE5MTQ0NDAwWjA7MQswCQYDVQQGEwJ0TDERMA8G  
A1UEChMIUG9sYXJ0TU0wGTAxBgNVBAMTEFBvbGFyU1NMIFRlc3QgQ0EwggEiMA0G  
CSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDA3zf8F7vglp0/ht6WMn1EpRagzSHx  
mdTs6st8GFgIlKXsm8WL3xoemTiZhX57wI053zhdcHgH057Zk+i5clHFzqMwUqny  
50BwFMtEonILwuVA+T7lpg6z+exKY8C4KQB0nFc7qKUEkHHxvYPZP9al4jwqj+8n  
YMPGn8u67GB9t+aEMr5P+1gmIgNb1LTV+/Xjli5ww0Quvfwu7uJBVcA0Ln0kcmnL  
R7EUQIN9Z/SG9jGr8XmksrUuEvmEF/Bibyc+ElixVA0hmnM3oTDPb5Lc9un8rNsu  
KNF+AksjoBXy0GVkCeoMbo4bF6BxyL0byavpw/LPh5aPgAIynplYb6LVAgMBAAGj  
gZUwgZIwDAYDVRR0TBAUwAwEB/zAdBgNVHQ4EFgQUtFrkpbPe0lL2udWmlQ/rPrzH  
/f8wYwYDVR0jBFwwWoAUtFrkpbPe0lL2udWmlQ/rPrzH/f+hP6Q9MDsxCzAJBgNV  
BAYTAk5MMREwDwYDVQQKEwhQb2xhcmlNTTDEZMBcGA1UEAxMQUG9sYXJ0TU0wGTAxBgNV  
dCBDAQIBADANBgkqhkiG9w0BAQUFAAOCQAQEAuP1U2ABUkIsIsCfdlc2i94QHHiYeJ  
SsR4EdgHtdciUI5I62J6Mom+Y0dT/7a+8S6MVMCZP6C5NyNyXw1GWY/YR82XTJ8H  
DBJiCTok5DbZ6Sza0NBzdWHXwwmi5vgldxn7YxrM9d0IjxM27WNKs4sDQhZBQkF  
pjmfs2cb4oPl4Y9T9meTx/lvdkRYEug61Jfn6cA+qHpyPYdTH+UshITnmp5/Ztkf  
m/UTSLBNFNHesiTZeh31NcxYGdHSme9Nc/gfidRa0FLOcfWxRlFqAI47zG9jAQCZ  
7Z2mCGDNMhjQc+BYcdnl0lPXjdDK6V0qCgldVewhUBcw5gZKzV7e9+DpVA==

-----END CERTIFICATE-----



```
PolarSSLTest
-----BEGIN CERTIFICATE-----
MIIDNzCCAhh+gAwIBAgIBAjANBgkqhkiG9w0BAQUFADA7MQswCQYDVQQGEwJOTDER
MA8GA1UEChMIUG9sYXJ0eWwGTAXBgNVBAMTEFBvbGFyU1NMIFRlc3QgQ0EwHhcN
MTEwMjE5MTQ0NDA2WhcNMjEwMjE5MTQ0NDA2WjA0MQswCQYDVQQGEwJOTDERMA8G
A1UEChMIUG9sYXJ0eWwEjAQBgNVBAMTCWxvY2FsaG9zdDCCASIwDQYJKoZIhvcN
AQEBBQADggEPADCCAQoCggEBAMFNo93nzR3RBNdJcriZrA545Do8Ss86ExbQWuTN
pWCip+4ea5anUrSQ7y1yej4kmvy2NKwk9XfgJmSMnLAofaHa6ozmyRyWvP7BBFKz
NtSj+uGxdtiQwWG0ZLI2oiZTqqt0Xgd9GYLbKtgfoNkNHC1JZvdbJXNG6AuKT2kM
tQCQ4dqCEGZ9rlQri2V5kaHiYcPNQEkI7mgM8YuG0ka/0LiqEQMef1aoGh5EGA8P
hYvai0Re4hjGYi/HZo36Xdh98yeJKQHFkA4/J/EwyEo079bex8cna8cFPXrEAjya
HT4P6DSYW8tzS1KW2BGiLICIaTla0w+w3lkvEcf36hIBMJcCAwEAAaNNMEswCQYD
VR0TBAlwADAdBgNVHQ4EFgQUpQXoZLjc32APUBJNYKhkr02LQ5MwHwYDVR0jBBgw
FoAutFrkpbPe0LL2udWmlQ/rPrzH/f8wDQYJKoZIhvcNAQEFBQADggEBAJxnXClY
pHkbp70cqBrsGXlybA74czb05RdLEgFs7rHVS9r+c293luS/KdliLScZqAZVylw
UfrWvKMoWhHYKp3dEIS4xTXk6/5zXxhv9Rw8SGc8qn6vITHk1S1mPevtekgasY5Y
iWQuM3h4YVLRH3HHEMAD1TnAexfXHHDFQGe+Bd1iAbz1/sH9H8l4StwX6egvTK3M
wXRwkKkvjKaEDA9ATbZx0mI8LGsxSuCqe9r9dyjmttd47J1p1Rulz3CLzaRcVIuS
RRQfaD8neM9c1S/iJ/amTVqJxA1K0d0S5780WhPfSArA+g4qAmSjelc3p4wWpha8
zhuYwjVuX6JHG0c=
-----END CERTIFICATE-----
```

## 2.5 CP-NVR-05: Static DH Parameters extracted (Reserved for : CVE-2024-54847)

Potential Impact : **High**

### Description :

During the assessment it was identified that the static hardcoded DH parameters were available in firmware

**Affected Hosts** : Device firmware, device identity, authentication.

### Steps to Reproduce:

- 1 Continue analyzing same file extracted by gnu strings.
- 2 DH parameters are available in same file.

```
-----BEGIN DH PARAMETERS-----  
MIGHAoGBAJ419DBE0gmQTzo5qXl5fQcN9TN455wkOL7052HzxxRVMyhYmwQcgJvh  
1sa18fyfR90iVEMYgl0pkqVoGLN7qd5aQNNi5W7/C+VBdHTBJcGZJyyP5B3qcz32  
9mLJKudlVudV0Qxk5qUJaPZ/xupz0NyoVpviuiB0IlgNi8ovSXWzAgEC  
-----END DH PARAMETERS-----
```

**##### End of Document #####**