Cisco IP Phone Cleartext Password Storage

Authored by Gerhard Hechenberger, Steffen Robertz | Site sec-consult.com

Posted Jan 17, 2022

Cisco IP Phone Series 78x1, 88x5, 88x1, 7832, 8832, 8821 and 3905 suffer from an insecure password storage vulnerability.

tags | exploit
systems | cisco
advisories | CVE-2022-20660
SHA-256 | 448c7c5cfcae3fc7bd414ad5be07cfbb1b7d955c723ac1c0f73d5e456f4c69e5 **Download** | **Favorite** | **View**

Related Files

Share This

Like 0 Tweet LinkedIn Reddit Digg StumbleUpon

Change Mirror Download

```
SEC Consult Vulnerability Lab Security Advisory < 20220113-0 >
=======================================================================
               title: Cleartext Storage of Phone Password
             product: Cisco IP Phone Series 78x1, 88x5, 88x1, 7832,
                      8832, 8821 and 3905
  vulnerable version: Firmware <14.1.1,
                      Firmware <11.0(6)SR2 (device model 8821),
                      Firmware <9.4(1)SR5 (device model 3905)
       fixed version: Firmware 14.1.1, 11.0(6)SR2, 9.4(1)SR5
          CVE number: CVE-2022-20660
              impact: Medium
            homepage: https://www.cisco.com
               found: 2021-04-15
                  by: Gerhard Hechenberger (Office Vienna)
                      Steffen Robertz (Office Vienna)
                      SEC Consult Vulnerability Lab

                      An integrated part of SEC Consult, an Atos company
                      Europe | Asia | North America

                      https://www.sec-consult.com

=======================================================================

Vendor description:
-------------------
"The Cisco® IP Phone 7800 Series is a cost-effective, high-fidelity voice
communications portfolio designed to improve your organization's people-centric
communications, while reducing your operating costs. It combines an attractive
new ergonomic design with "always-on" reliability and secure encrypted
communications. The Cisco® IP Phone 7800 Series delivers advanced IP Telephony
features and crystal clear wideband audio performance to deliver an
easy-to-use, full-featured voice communications experience on Cisco on-premises
and hosted infrastructure platforms and third party hosted call control."

Source: https://www.cisco.com/c/en/us/products/collateral/collaboration-endpoints/unified-ip-phone-7800-
series/data-sheet-c78-729488.html


Business recommendation:
------------------------
SEC Consult recommends to update the devices to the newest firmware listed
below, where, according to the vendor, the documented issue is fixed.

We want to thank Cisco for the very professional response and great coordination.


Vulnerability overview/description:
-----------------------------------
1) Cleartext Storage of Phone Password
The phone is storing the "phone password", which is needed to access its
administrative settings, in cleartext (in multiple locations) in the flash
memory.

Because the password is not hashed using a suitable cryptographic hash function
and the storage is unencrypted, a physical attacker can easily recover the
password and reuse it on other phones, if they are not configured to use unique
administrative passwords.


Proof of concept:
-----------------
1) Cleartext Storage of Phone Password
Steps to take:
- Configure a phone password via the TFTP XML provisioning feature.
- Desoldering the memory and reading its content.
- Analyzing the memory content. As example, the Linux command 'strings' can be
  used below to show the identified password in cleartext in the dumped data.
   ---------------------------------------
   $ strings nand.dump | grep phonePassword
   phonePassword>sectest</,x
```

Follow us on Twitter

Subscribe to an RSS Feed

File Archive: November 2022 <

Su	Mo	Tu	We	Th	Fr	Sa
		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30			

Top Authors In Last 30 Days

Red Hat 186 files
Ubuntu 52 files
Gentoo 44 files
Debian 27 files
Apple 25 files
Google Security Research 14 files
malvuln 10 files
nu11secur1ty 6 files
mjurczyk 4 files
George Tsimpidas 3 files

File Tags

ActiveX (932)
Advisory (79,557)
Arbitrary (15,643)
BBS (2,859)
Bypass (1,615)
CGI (1,015)
Code Execution (6,913)
Conference (672)
Cracker (840)
CSRF (3,288)
DoS (22,541)
Encryption (2,349)
Exploit (50,293)
File Inclusion (4,162)
File Upload (946)
Firewall (821)
Info Disclosure (2,656)

File Archives

November 2022
October 2022
September 2022
August 2022
July 2022
June 2022
May 2022
April 2022
March 2022
February 2022
January 2022
December 2021
Older

Systems

AIX (426)
Apple (1,926)

```
   phonePassword>sectest</,x
   phonePassword>sectest</,x
   phonePassword>sectest</,x
   ----------------------------------------


Vulnerable / tested versions:
-----------------------------
The following firmware/device has been tested:
* Cisco IP Phone 7821: Firmware version 12.8.1-0001-455

The vendor confirmed that the following devices are affected:
* Cisco IP Phone 78x1 all releases before firmware version 14.1.1
* Cisco IP Phone 88x5 all releases before firmware version 14.1.1
* Cisco IP Phone 88x1 all releases before firmware version 14.1.1
* Cisco IP Phone 7832 all releases before firmware version 14.1.1
* Cisco IP Phone 8832 all releases before firmware version 14.1.1
* Cisco IP Phone 8821 all releases before firmware version 11.0(6)SR2
* Cisco IP Phone 3905 all releases before firmware version 9.4(1)SR5


Vendor contact timeline:
------------------------
2021-05-19: Contacting vendor through psirt@cisco.com. Set preliminary release
            date to 2021-08-07. Received PSIRT case number from Cisco employee.
2021-05-20: Cisco states that the finding has been shared with the development
            team and is currently being analyzed.
2021-06-30: Cisco confirms affected phone models and communicates expected
            dates for fixed firmware releases.
2021-07-07: New estimated release date was set to 2022-01-31.
2021-12-27: Cisco informs about the fix and the publishing date 2022-01-12 for
            their advisory
2022-01-13: Coordinated release of the security advisory.



Solution:
---------
Update the firmware of the affected devices to the latest available version.
See the vendor's security advisory for further information.

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ip-phone-info-disc-fRdJfOxA


Workaround:
-----------
For immediate mitigation, ensure that phones are configured to use unique
administrative passwords.


Advisory URL:
-------------
https://sec-consult.com/vulnerability-lab/


~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

SEC Consult Vulnerability Lab

SEC Consult, an Atos company
Europe | Asia | North America

About SEC Consult Vulnerability Lab
The SEC Consult Vulnerability Lab is an integrated part of SEC Consult, an
Atos company. It ensures the continued knowledge gain of SEC Consult in the
field of network and application security to stay ahead of the attacker. The
SEC Consult Vulnerability Lab supports high-quality penetration testing and
the evaluation of new offensive and defensive technologies for our customers.
Hence our customers obtain the most current information about vulnerabilities
and valid recommendation about the risk profile of new technologies.

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
Interested to work with the experts of SEC Consult?
Send us your application https://sec-consult.com/career/

Interested in improving your cyber security with the experts of SEC Consult?
Contact our local offices https://sec-consult.com/contact/
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

Mail: research at sec-consult dot com
Web: https://www.sec-consult.com
Blog: http://blog.sec-consult.com
Twitter: https://twitter.com/sec_consult

EOF Gerhard Hechenberger, Steffen Robertz / @2022
```

Intrusion Detection	(866)	BSD	(370)
Java	(2,888)	CentOS	(55)
JavaScript	(817)	Cisco	(1,917)
Kernel	(6,255)	Debian	(6,620)
Local	(14,173)	Fedora	(1,690)
Magazine	(586)	FreeBSD	(1,242)
Overflow	(12,390)	Gentoo	(4,272)
Perl	(1,417)	HPUX	(878)
PHP	(5,087)	iOS	(330)
Proof of Concept	(2,290)	iPhone	(108)
Protocol	(3,426)	IRIX	(220)
Python	(1,449)	Juniper	(67)
Remote	(30,009)	Linux	(44,118)
Root	(3,496)	Mac OS X	(684)
Ruby	(594)	Mandriva	(3,105)
Scanner	(1,631)	NetBSD	(255)
Security Tool	(7,768)	OpenBSD	(479)
Shell	(3,098)	RedHat	(12,339)
Shellcode	(1,204)	Slackware	(941)
Sniffer	(885)	Solaris	(1,607)
Spoof	(2,165)	SUSE	(1,444)
SQL Injection	(16,089)	Ubuntu	(8,147)
TCP	(2,377)	UNIX	(9,150)
Trojan	(685)	UnixWare	(185)
UDP	(875)	Windows	(6,504)
Virus	(661)	Other	
Vulnerability	(31,104)		
Web	(9,329)		
Whitepaper	(3,728)		
x86	(946)		
XSS	(17,478)		
Other			

Login or Register to add favorites

Site Links
- News by Month
- News Tags
- Files by Month
- File Tags
- File Directory

About Us
- History & Purpose
- Contact Information
- Terms of Service
- Privacy Statement
- Copyright Information

Hosting By
- Rokasec

Follow us on Twitter

Subscribe to an RSS Feed