RoyalTS SSH Tunnel Authentication Bypass

Authored by Michele Toccagni

Posted Jun 9, 2020

RoyalTS SSH Tunnel versions prior to 5 for Windows suffer from an authentication bypass vulnerability.

tags | advisory, bypass
systems | windows
advisories | CVE-2020-13872
SHA-256 | 1a8db84c812d8d110796638e2e38f42e172e4cb2bfb9498b798176f53999e5e2 **Download** | **Favorite** | **View**

Related Files

Share This

Like Twee LinkedIn Reddit Digg StumbleUpon

Change Mirror Download

```
RoyalTS SSH Tunnel - Authentication Bypass
================================================================================

Identifiers
-------------------------------------------------
* CVE-2020-13872


CVSSv3 score
-------------------------------------------------
8.8 - [AV:A/AC:L/PR:N/UI:N/S:C/C:H/I:L/A:L](
https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?vector=AV:A/AC:L/PR:N/UI:N/S:C/C:H/I:L/A:L&version=3.1
)


Vendor
-------------------------------------------------
RoyalApps - https://www.royalapps.com/


Product
-------------------------------------------------
Royal TS provides powerful, easy and secure access to your remote
systems.
It's the perfect tool for server admins, system engineers, developers
and IT focused information workers
who constantly need to access remote systems with different protocols
(like RDP, VNC, SSH, HTTP/S, and many more.).


Affected versions
-------------------------------------------------
  - All versions prior to RoyalTS v5 for Windows.


Credit
-------------------------------------------------
Michele Toccagni - toccagni.info


Vulnerability summary
-------------------------------------------------
This vulnerability allows a remote attackers to bypass the
authentication of the tunnel
and gain access to an internal network. The problem is that, once a
SSH tunnel is created on the bridge host with a Secure Gateway, this
tunnel will listen on the address 0.0.0.0 on the port opened ad hoc by
RoyalTS (higher than 50000), leaving the possibility for anyone to
exploit the tunnel without having to authenticate to it.
The attacker could easily bruteforce the ssh/rdp login in the internal
network, or,
even worse, if the hosts aren't patched, could use some known exploits
and perform lateral movements.
The vulnerability is fixed in the current major release (Royal TS V5).



Proof of concept
-------------------------------------------------
I wrote a detailed blog post to explain the bug:
https://hacktips.it/royalts-ssh-tunnel-authentication-bypass/

Solution
-------------------------------------------------
Upgrade to RoyalTS V5 for Windows

Timeline
-------------------------------------------------
Date        | Status
------------|---------------------
04-JUN-2020 | Reported to vendor
04-JUN-2020 | Vendor replied that it's a known bug and it's fixed on the
last major version
06-JUN-2020 | CVE assigned
08-JUN-2020 | Public disclosure
```

Login or Register to add favorites

Follow us on Twitter

Subscribe to an RSS Feed

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)

Spoof (2,166)
SQL Injection (16,102)
TCP (2,379)
Trojan (686)
UDP (876)
Virus (662)
Vulnerability (31,136)
Web (9,365)
Whitepaper (3,729)
x86 (946)
XSS (17,494)
Other

SUSE (1,444)
Ubuntu (8,199)
UNIX (9,159)
UnixWare (185)
Windows (6,511)
Other

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