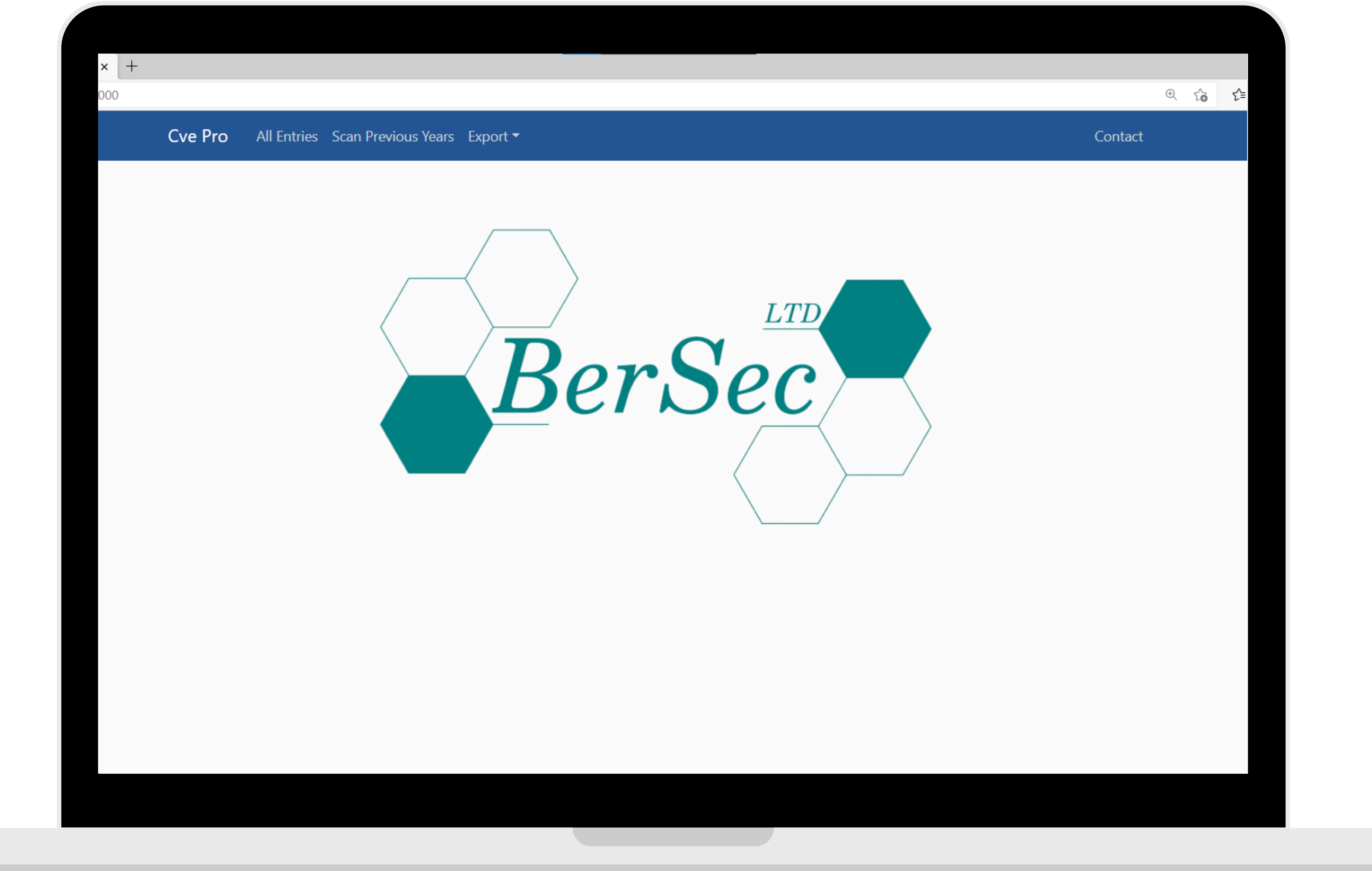
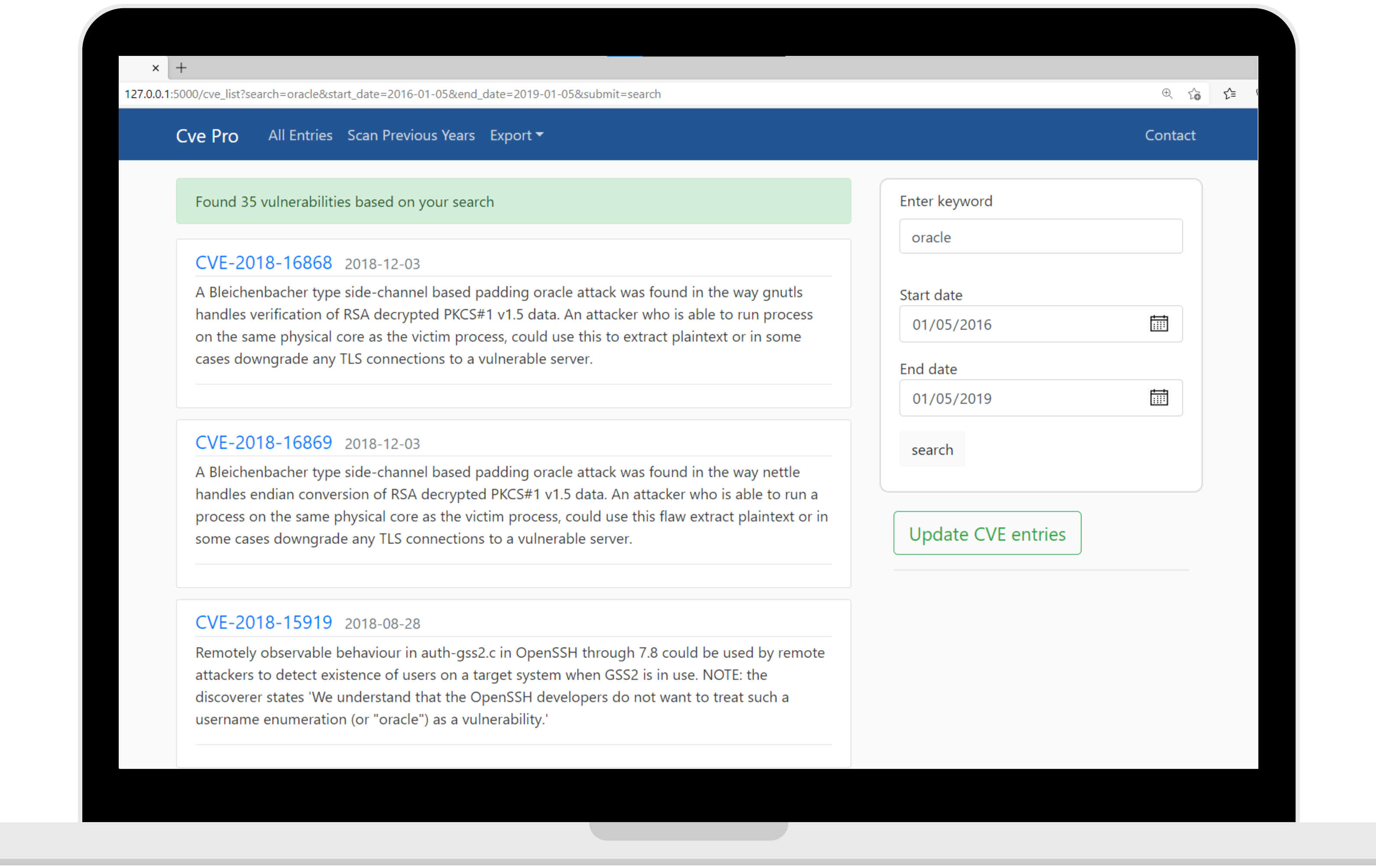
HOMEPAGE



SEARCH PAGE WITH KEYWORD AND DATE RANGE FILTERS



127.0.0.1:5000/cve_list?search=oracle&start_date=2016-01-05&end_date=2019-01-05&submit=search

Found 35 vulnerabilities based on your search

CVE-2018-16868 2018-12-03

A Bleichenbacher type side-channel based padding oracle attack was found in the way gnutls handles verification of RSA decrypted PKCS#1 v1.5 data. An attacker who is able to run process on the same physical core as the victim process, could use this to extract plaintext or in some cases downgrade any TLS connections to a vulnerable server.

CVE-2018-16869 2018-12-03

A Bleichenbacher type side-channel based padding oracle attack was found in the way nettle handles endian conversion of RSA decrypted PKCS#1 v1.5 data. An attacker who is able to run a process on the same physical core as the victim process, could use this flaw extract plaintext or in some cases downgrade any TLS connections to a vulnerable server.

CVE-2018-15919 2018-08-28

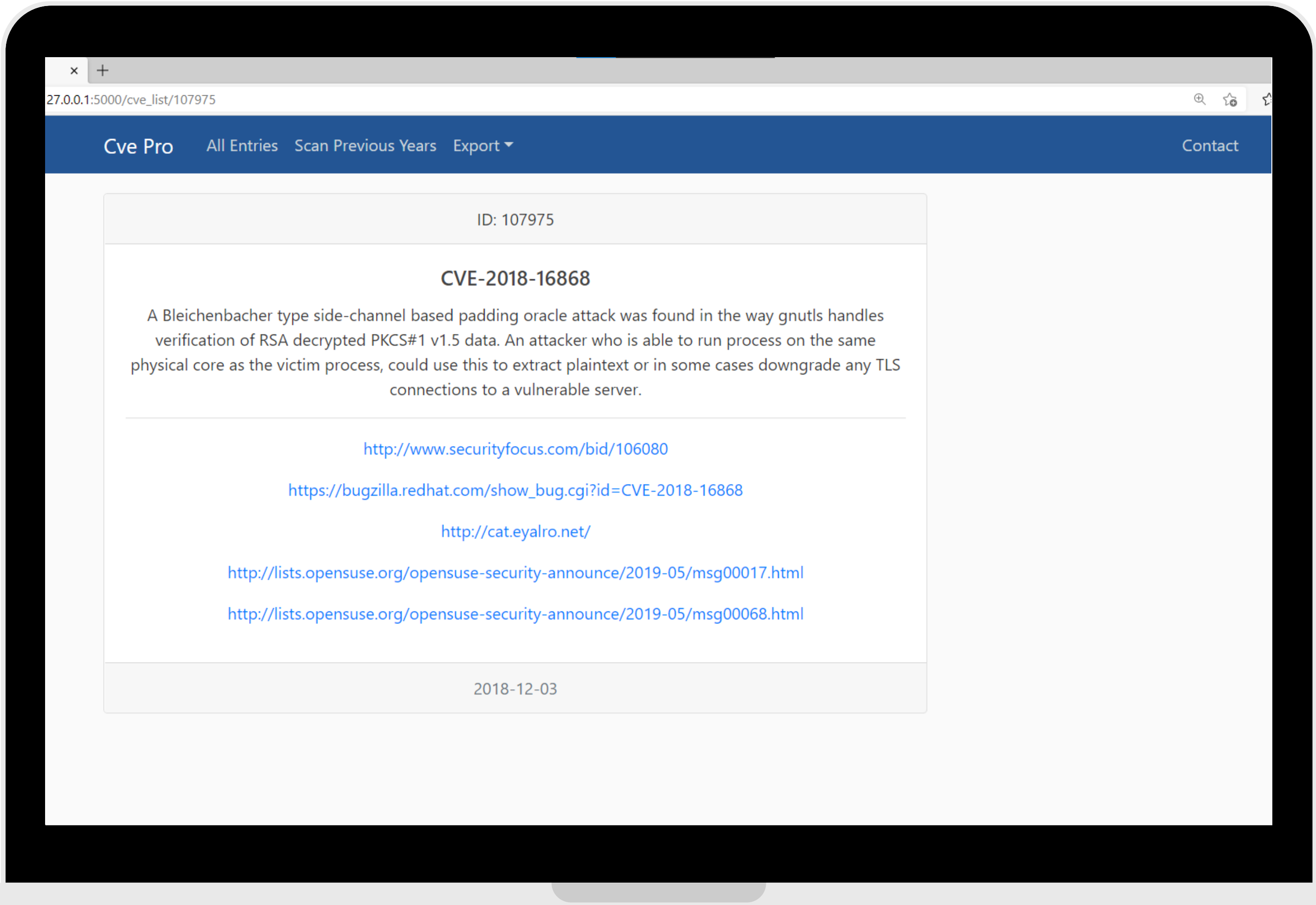
Remotely observable behaviour in auth-gss2.c in OpenSSH through 7.8 could be used by remote attackers to detect existence of users on a target system when GSS2 is in use. NOTE: the discoverer states 'We understand that the OpenSSH developers do not want to treat such a username enumeration (or "oracle") as a vulnerability.'

Enter keyword: oracle

Start date: 01/05/2016

End date: 01/05/2019

DETAIL PAGE FOR EACH CVE, CONTAINS ALL ITS REFERENCES



ID: 107975

CVE-2018-16868

A Bleichenbacher type side-channel based padding oracle attack was found in the way gnutls handles verification of RSA decrypted PKCS#1 v1.5 data. An attacker who is able to run process on the same physical core as the victim process, could use this to extract plaintext or in some cases downgrade any TLS connections to a vulnerable server.

http://www.securityfocus.com/bid/106080

https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2018-16868

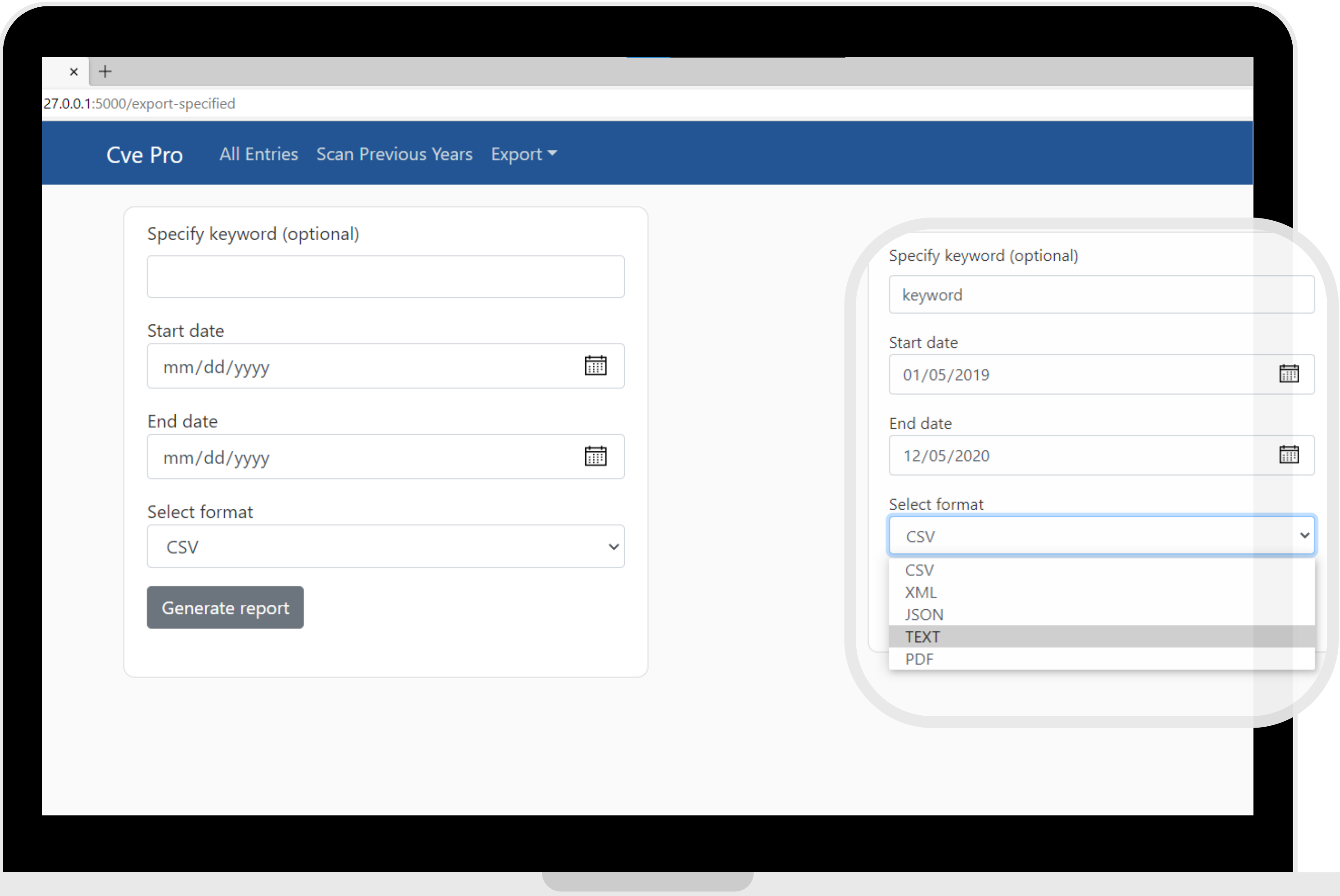
http://cat.eyalro.net/

http://lists.opensuse.org/opensuse-security-announce/2019-05/msg00017.html

http://lists.opensuse.org/opensuse-security-announce/2019-05/msg00068.html

2018-12-03

EXPORT PAGE (CSV, PDF, XML, JSON, TEXT)



Specify keyword (optional)

Start date

mm/dd/yyyy

End date

mm/dd/yyyy

Select format

CSV

Specify keyword (optional)

keyword

Start date

01/05/2019

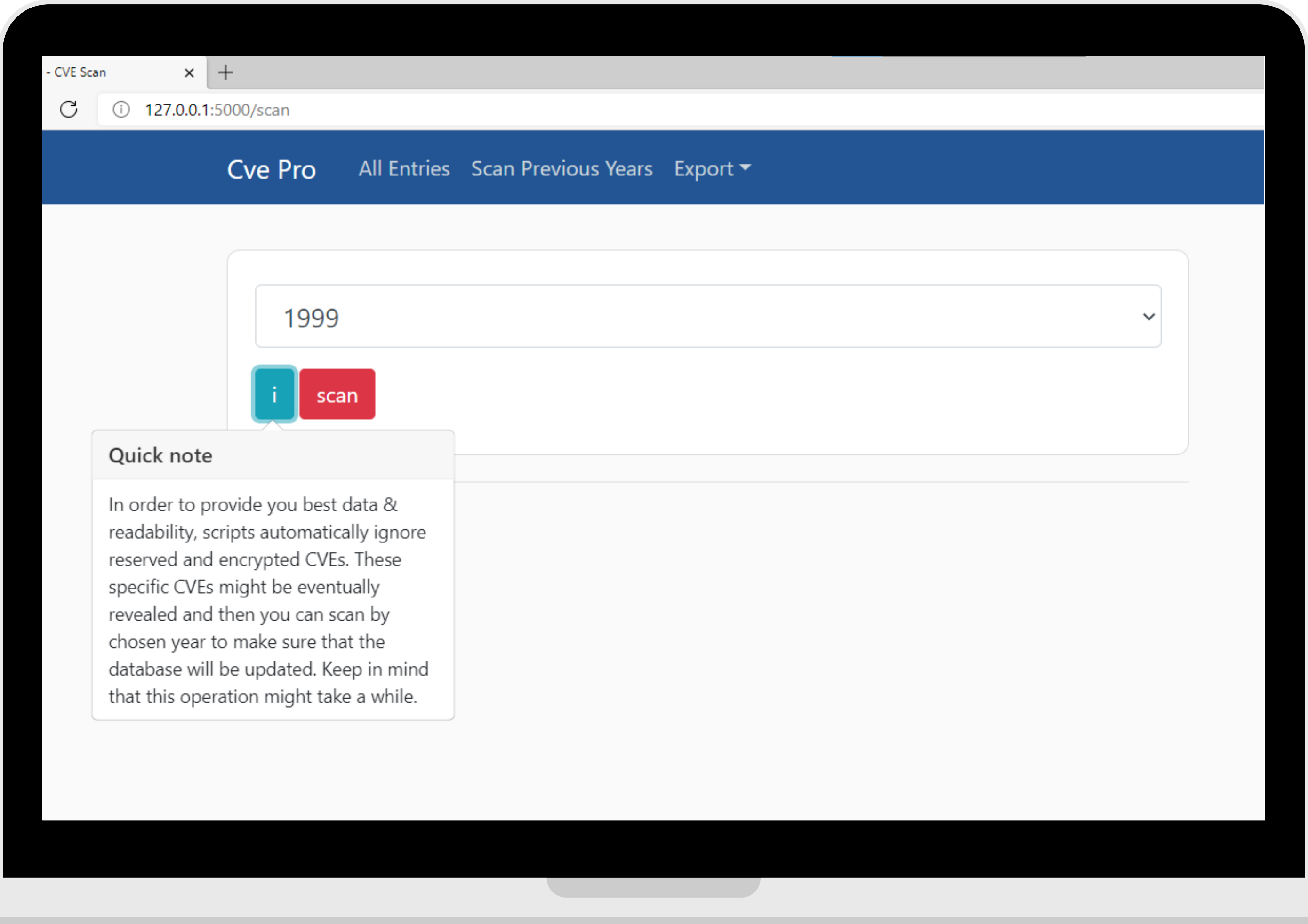
End date

12/05/2020

Select format

CSV

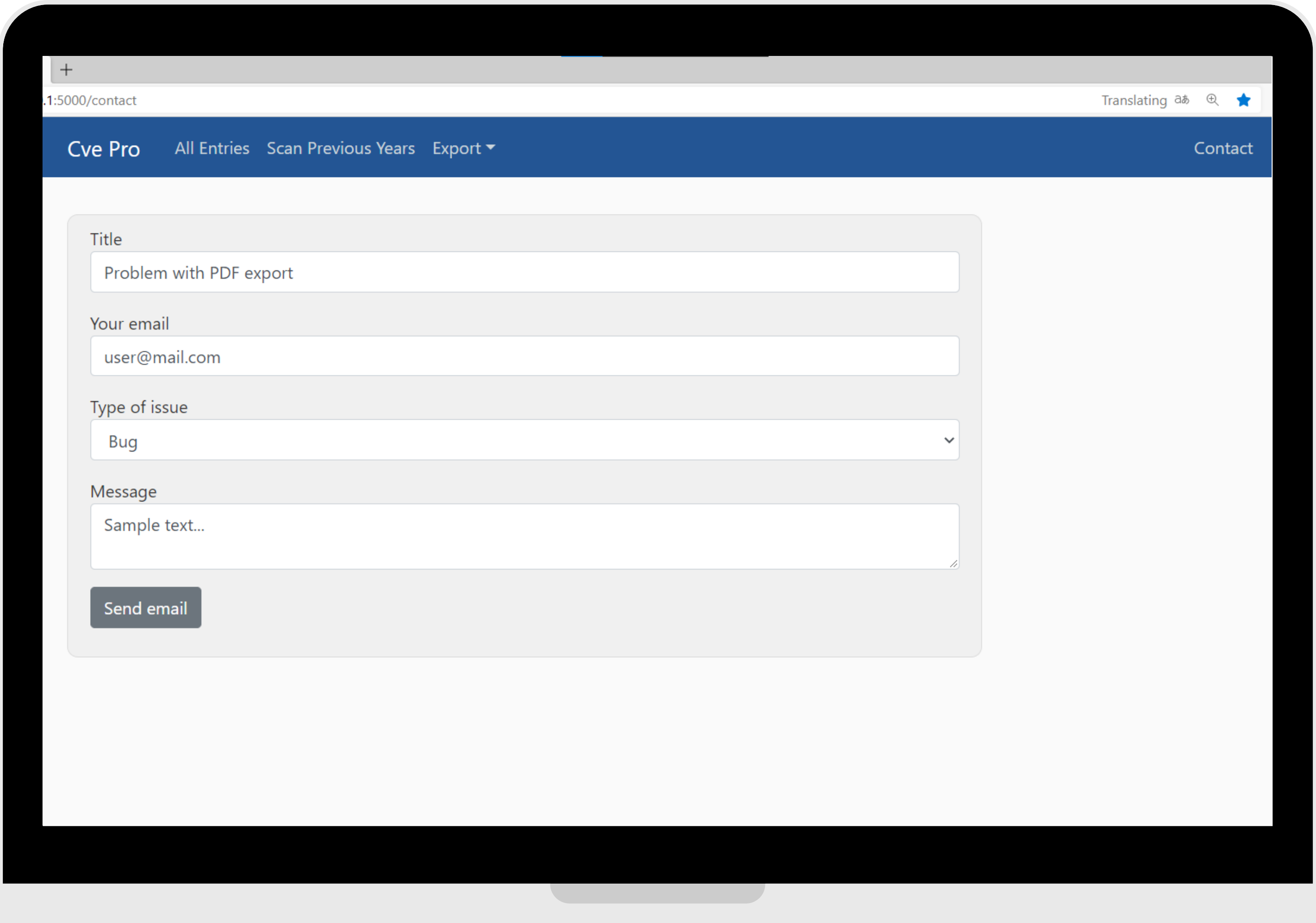
SCANNING SPECIFIC YEAR FOR MISSING VULNERABILITIES



Quick note

In order to provide you best data & readability, scripts automatically ignore reserved and encrypted CVEs. These specific CVEs might be eventually revealed and then you can scan by chosen year to make sure that the database will be updated. Keep in mind that this operation might take a while.

SUPPORT CONTACT



Title: Problem with PDF export

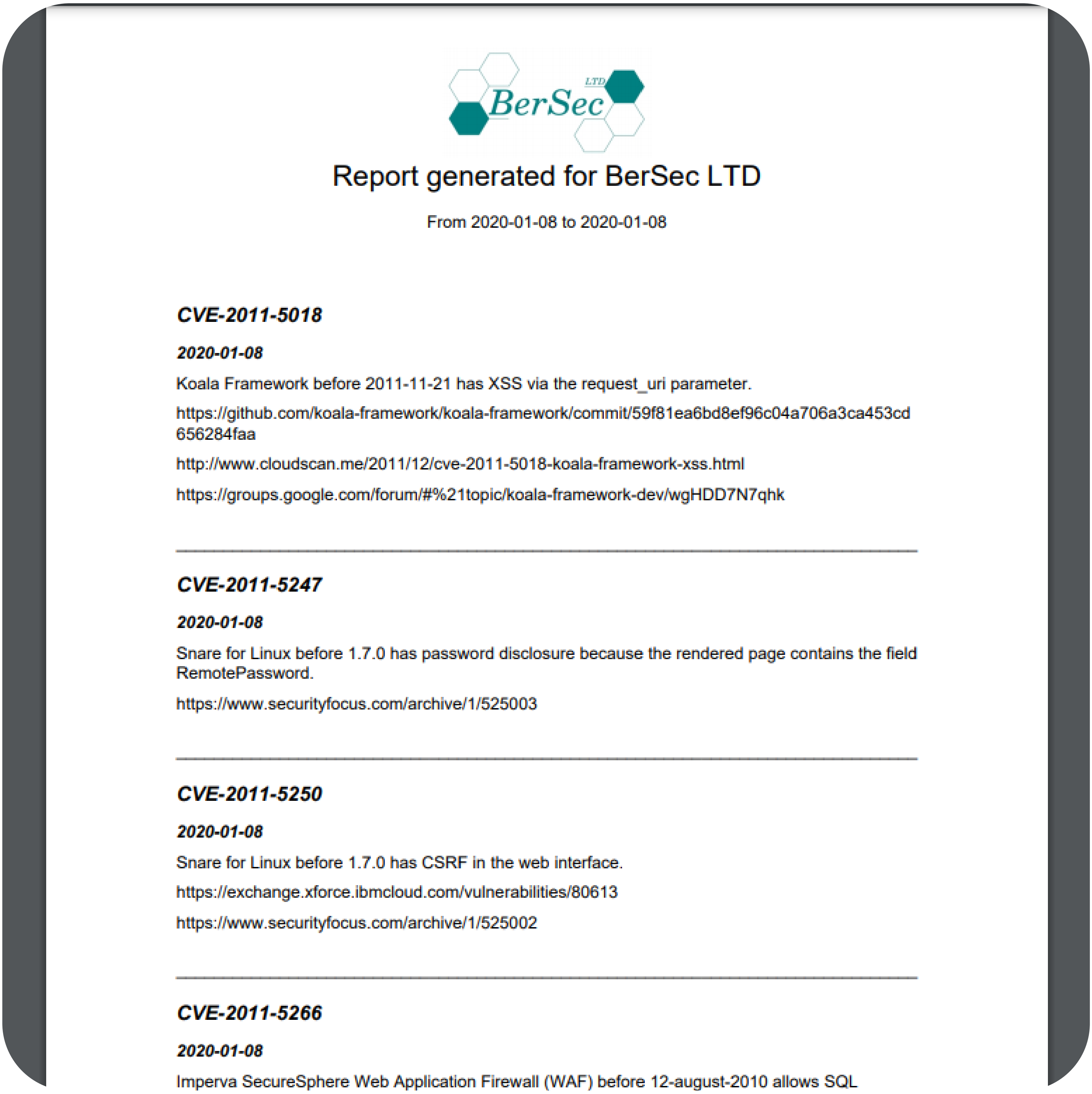
Your email: user@mail.com

Type of issue: Bug

Message: Sample text...

Reports generated by application:

PDF



Report generated for BerSec LTD

From 2020-01-08 to 2020-01-08

CVE-2011-5018

2020-01-08

Koala Framework before 2011-11-21 has XSS via the request_uri parameter.

https://github.com/koala-framework/koala-framework/commit/59f81ea6bd8ef96c04a706a3ca453cd656284faa

http://www.cloudscan.me/2011/12/cve-2011-5018-koala-framework-xss.html

https://groups.google.com/forum/#%21topic/koala-framework-dev/wgHDD7N7qhk

---

CVE-2011-5247

2020-01-08

Snare for Linux before 1.7.0 has password disclosure because the rendered page contains the field RemotePassword.

https://www.securityfocus.com/archive/1/525003

CVE-2011-5250

2020-01-08

Snare for Linux before 1.7.0 has CSRF in the web interface.

https://exchange.xforce.ibmcloud.com/vulnerabilities/80613

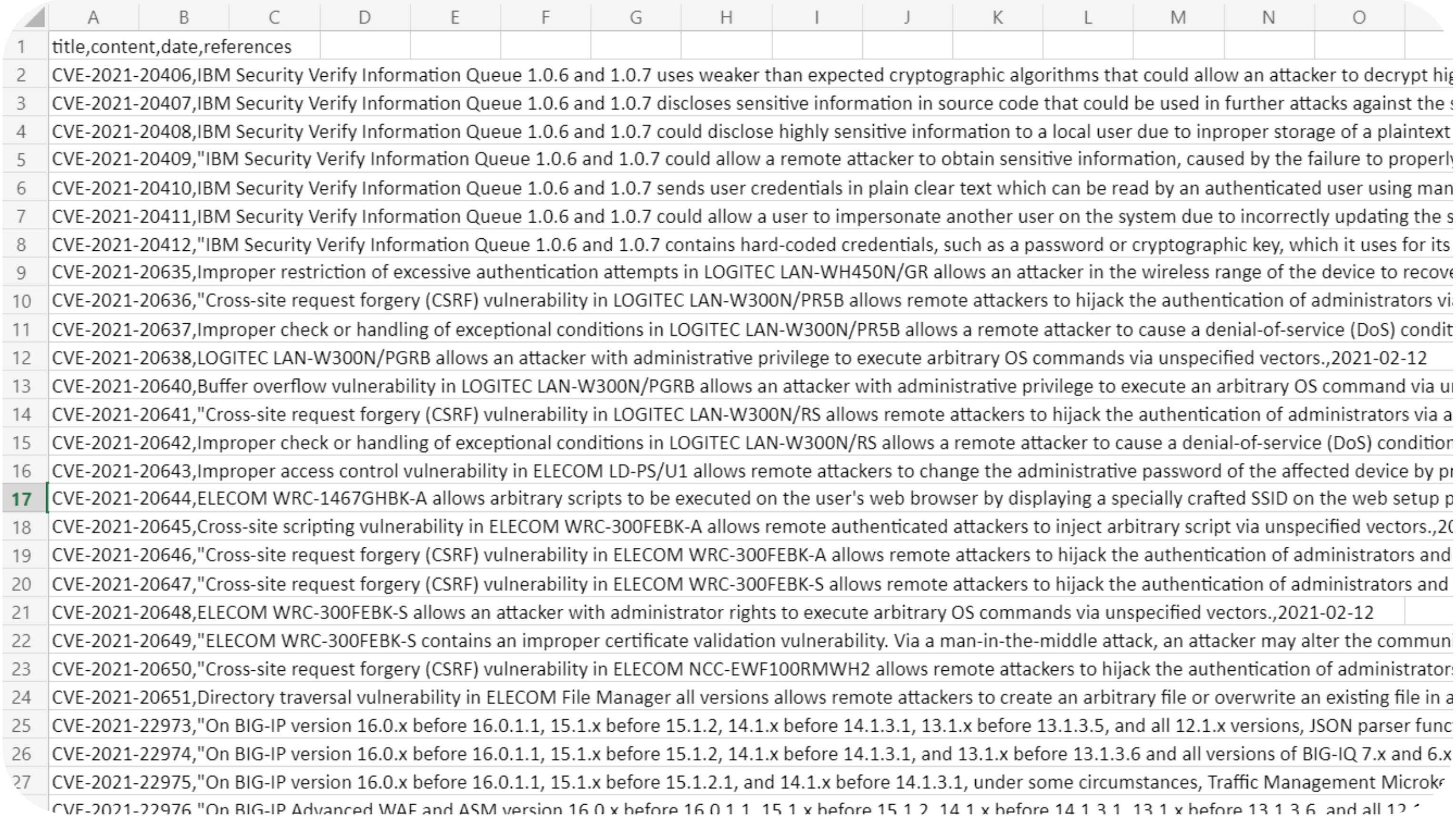
https://www.securityfocus.com/archive/1/525002

CVE-2011-5266

2020-01-08

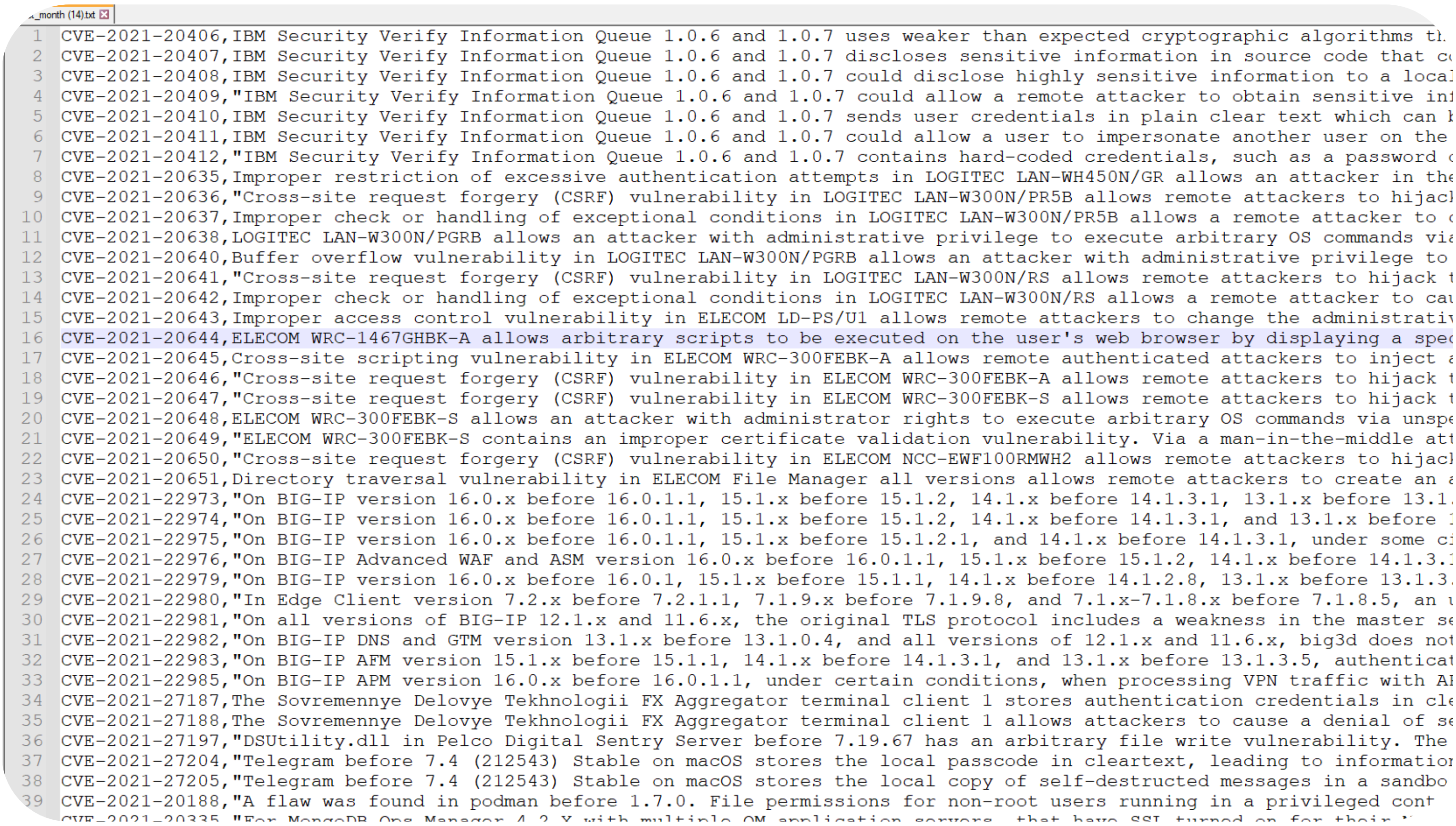
Imperva SecureSphere Web Application Firewall (WAF) before 12-august-2010 allows SQL

CSV



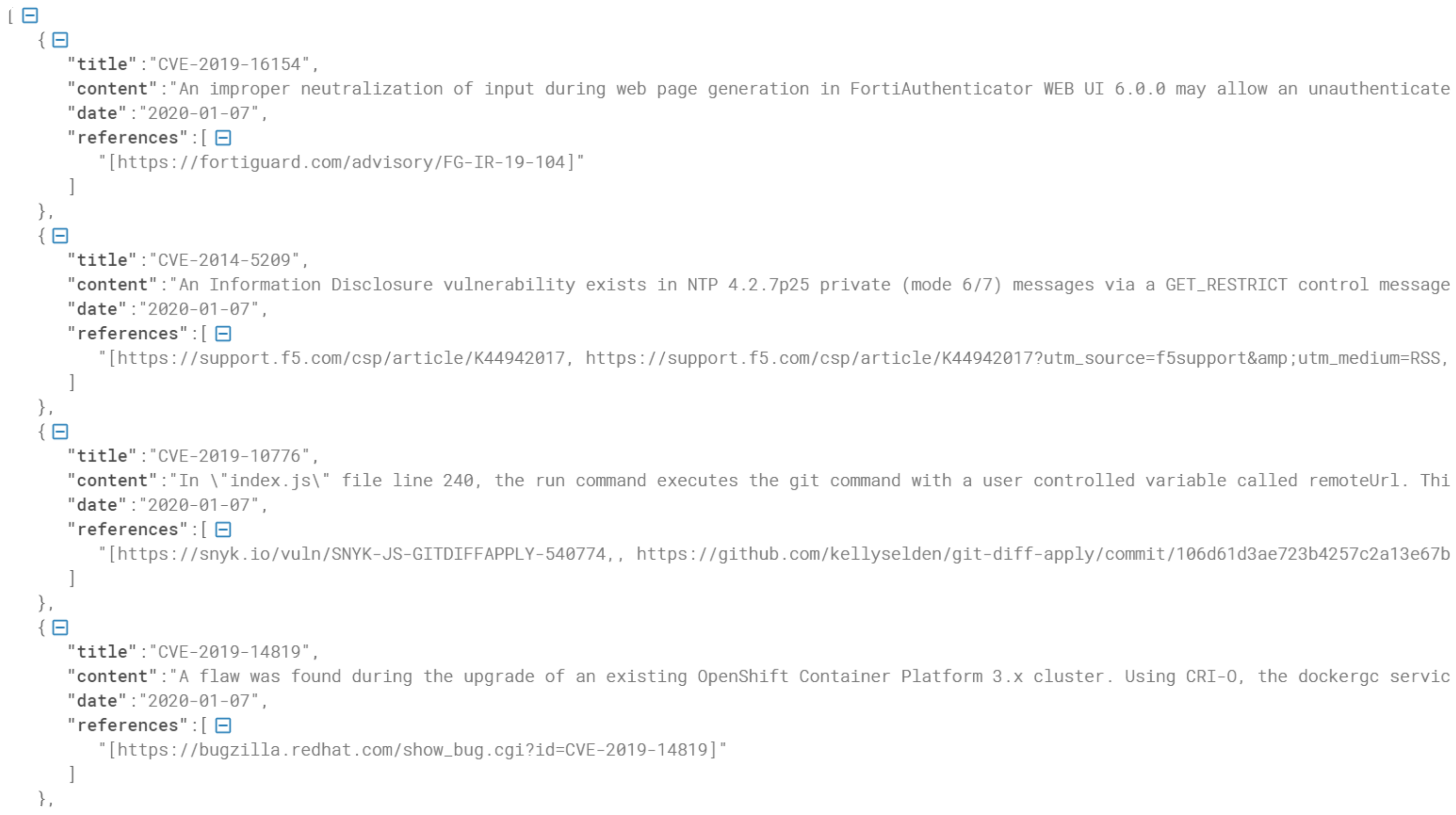
```
title,content,date,references
CVE-2021-20406,IBM Security Verify Information Queue 1.0.6 and 1.0.7 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt hig
CVE-2021-20407,IBM Security Verify Information Queue 1.0.6 and 1.0.7 discloses sensitive information in source code that could be used in further attacks against the s
CVE-2021-20408,IBM Security Verify Information Queue 1.0.6 and 1.0.7 could disclose highly sensitive information to a local user due to inproper storage of a plaintext
CVE-2021-20409,"IBM Security Verify Information Queue 1.0.6 and 1.0.7 could allow a remote attacker to obtain sensitive information, caused by the failure to properly
CVE-2021-20410,IBM Security Verify Information Queue 1.0.6 and 1.0.7 sends user credentials in plain clear text which can be read by an authenticated user using man
CVE-2021-20411,IBM Security Verify Information Queue 1.0.6 and 1.0.7 could allow a user to impersonate another user on the system due to incorrectly updating the s
CVE-2021-20412,"IBM Security Verify Information Queue 1.0.6 and 1.0.7 contains hard-coded credentials, such as a password or cryptographic key, which it uses for its
CVE-2021-20635,Improper restriction of excessive authentication attempts in LOGITEC LAN-WH450N/GR allows an attacker in the wireless range of the device to recove
CVE-2021-20636,"Cross-site request forgery (CSRF) vulnerability in LOGITEC LAN-W300N/PR5B allows remote attackers to hijack the authentication of administrators vi
CVE-2021-20637,Improper check or handling of exceptional conditions in LOGITEC LAN-W300N/PR5B allows a remote attacker to cause a denial-of-service (DoS) condit
CVE-2021-20638,LOGITEC LAN-W300N/PGRB allows an attacker with administrative privilege to execute arbitrary OS commands via unspecified vectors.,2021-02-12
CVE-2021-20640,Buffer overflow vulnerability in LOGITEC LAN-W300N/PGRB allows an attacker with administrative privilege to execute an arbitrary OS command via u
CVE-2021-20641,"Cross-site request forgery (CSRF) vulnerability in LOGITEC LAN-W300N/RS allows remote attackers to hijack the authentication of administrators via a
CVE-2021-20642,Improper check or handling of exceptional conditions in LOGITEC LAN-W300N/RS allows a remote attacker to cause a denial-of-service (DoS) condition
CVE-2021-20643,Improper access control vulnerability in ELECOM LD-PS/U1 allows remote attackers to change the administrative password of the affected device by pr
CVE-2021-20644,ELECOM WRC-1467GHBK-A allows arbitrary scripts to be executed on the user's web browser by displaying a specially crafted SSID on the web setup p
CVE-2021-20645,Cross-site scripting vulnerability in ELECOM WRC-300FEBK-A allows remote authenticated attackers to inject arbitrary script via unspecified vectors.,20
CVE-2021-20646,"Cross-site request forgery (CSRF) vulnerability in ELECOM WRC-300FEBK-A allows remote attackers to hijack the authentication of administrators and
CVE-2021-20647,"Cross-site request forgery (CSRF) vulnerability in ELECOM WRC-300FEBK-S allows remote attackers to hijack the authentication of administrators and
CVE-2021-20648,ELECOM WRC-300FEBK-S allows an attacker with administrator rights to execute arbitrary OS commands via unspecified vectors.,2021-02-12
CVE-2021-20649,"ELECOM WRC-300FEBK-S contains an improper certificate validation vulnerability. Via a man-in-the-middle attack, an attacker may alter the communi
CVE-2021-20650,"Cross-site request forgery (CSRF) vulnerability in ELECOM NCC-EWF100RMWH2 allows remote attackers to hijack the authentication of administrator
CVE-2021-20651,Directory traversal vulnerability in ELECOM File Manager all versions allows remote attackers to create an arbitrary file or overwrite an existing file in a
CVE-2021-22973,"On BIG-IP version 16.0.x before 16.0.1.1, 15.1.x before 15.1.2, 14.1.x before 14.1.3.1, 13.1.x before 13.1.3.5, and all 12.1.x versions, JSON parser func
CVE-2021-22974,"On BIG-IP version 16.0.x before 16.0.1.1, 15.1.x before 15.1.2, 14.1.x before 14.1.3.1, and 13.1.x before 13.1.3.6 and all versions of BIG-IQ 7.x and 6.x
CVE-2021-22975,"On BIG-IP version 16.0.x before 16.0.1.1, 15.1.x before 15.1.2.1, and 14.1.x before 14.1.3.1, under some circumstances, Traffic Management Microk
CVE-2021-22976,"On BIG-IP Advanced WAF and ASM version 16.0.x before 16.0.1.1, 15.1.x before 15.1.2, 14.1.x before 14.1.3.1, 13.1.x before 13.1.3.6, and all 12.
```

TEXT



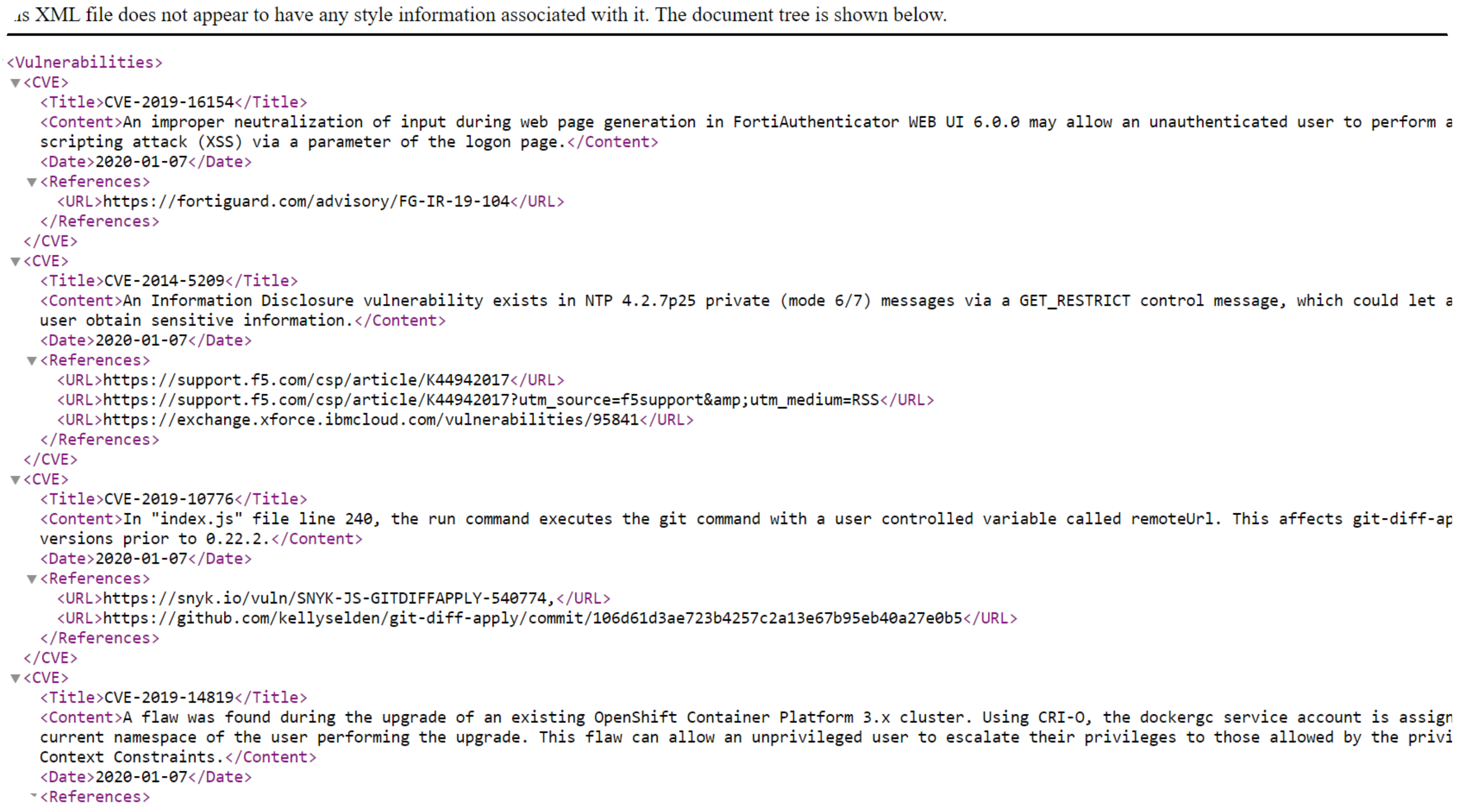
```
CVE-2021-20406,IBM Security Verify Information Queue 1.0.6 and 1.0.7 uses weaker than expected cryptographic algorithms th
CVE-2021-20407,IBM Security Verify Information Queue 1.0.6 and 1.0.7 discloses sensitive information in source code that co
CVE-2021-20408,IBM Security Verify Information Queue 1.0.6 and 1.0.7 could disclose highly sensitive information to a local
CVE-2021-20409,"IBM Security Verify Information Queue 1.0.6 and 1.0.7 could allow a remote attacker to obtain sensitive inf
CVE-2021-20410,IBM Security Verify Information Queue 1.0.6 and 1.0.7 sends user credentials in plain clear text which can b
CVE-2021-20411,IBM Security Verify Information Queue 1.0.6 and 1.0.7 could allow a user to impersonate another user on the
CVE-2021-20412,"IBM Security Verify Information Queue 1.0.6 and 1.0.7 contains hard-coded credentials, such as a password o
CVE-2021-20635,Improper restriction of excessive authentication attempts in LOGITEC LAN-WH450N/GR allows an attacker in the
CVE-2021-20636,"Cross-site request forgery (CSRF) vulnerability in LOGITEC LAN-W300N/PR5B allows remote attackers to hijack
CVE-2021-20637,Improper check or handling of exceptional conditions in LOGITEC LAN-W300N/PR5B allows a remote attacker to c
CVE-2021-20638,LOGITEC LAN-W300N/PGRB allows an attacker with administrative privilege to execute arbitrary OS commands via
CVE-2021-20640,Buffer overflow vulnerability in LOGITEC LAN-W300N/PGRB allows an attacker with administrative privilege to
CVE-2021-20641,"Cross-site request forgery (CSRF) vulnerability in LOGITEC LAN-W300N/RS allows remote attackers to hijack t
CVE-2021-20642,Improper check or handling of exceptional conditions in LOGITEC LAN-W300N/RS allows a remote attacker to cau
CVE-2021-20643,Improper access control vulnerability in ELECOM LD-PS/U1 allows remote attackers to change the administrativ
CVE-2021-20644,ELECOM WRC-1467GHBK-A allows arbitrary scripts to be executed on the user's web browser by displaying a spec
CVE-2021-20645,Cross-site scripting vulnerability in ELECOM WRC-300FEBK-A allows remote authenticated attackers to inject a
CVE-2021-20646,"Cross-site request forgery (CSRF) vulnerability in ELECOM WRC-300FEBK-A allows remote attackers to hijack t
CVE-2021-20647,"Cross-site request forgery (CSRF) vulnerability in ELECOM WRC-300FEBK-S allows remote attackers to hijack t
CVE-2021-20648,ELECOM WRC-300FEBK-S allows an attacker with administrator rights to execute arbitrary OS commands via unspe
CVE-2021-20649,"ELECOM WRC-300FEBK-S contains an improper certificate validation vulnerability. Via a man-in-the-middle att
CVE-2021-20650,"Cross-site request forgery (CSRF) vulnerability in ELECOM NCC-EWF100RMWH2 allows remote attackers to hijack
CVE-2021-20651,Directory traversal vulnerability in ELECOM File Manager all versions allows remote attackers to create an a
CVE-2021-22973,"On BIG-IP version 16.0.x before 16.0.1.1, 15.1.x before 15.1.2, 14.1.x before 14.1.3.1, 13.1.x before 13.1.
CVE-2021-22974,"On BIG-IP version 16.0.x before 16.0.1.1, 15.1.x before 15.1.2, 14.1.x before 14.1.3.1, and 13.1.x before 1
CVE-2021-22975,"On BIG-IP version 16.0.x before 16.0.1.1, 15.1.x before 15.1.2.1, and 14.1.x before 14.1.3.1, under some ci
CVE-2021-22976,"On BIG-IP Advanced WAF and ASM version 16.0.x before 16.0.1.1, 15.1.x before 15.1.2, 14.1.x before 14.1.3.1
CVE-2021-22979,"On BIG-IP version 16.0.x before 16.0.1, 15.1.x before 15.1.1, 14.1.x before 14.1.2.8, 13.1.x before 13.1.3.
CVE-2021-22980,"In Edge Client version 7.2.x before 7.2.1.1, 7.1.9.x before 7.1.9.8, and 7.1.x-7.1.8.x before 7.1.8.5, an u
CVE-2021-22981,"On all versions of BIG-IP 12.1.x and 11.6.x, the original TLS protocol includes a weakness in the master se
CVE-2021-22982,"On BIG-IP DNS and GTM version 13.1.x before 13.1.0.4, and all versions of 12.1.x and 11.6.x, big3d does not
CVE-2021-22983,"On BIG-IP AFM version 15.1.x before 15.1.1, 14.1.x before 14.1.3.1, and 13.1.x before 13.1.3.5, authenticat
CVE-2021-22985,"On BIG-IP APM version 16.0.x before 16.0.1.1, under certain conditions, when processing VPN traffic with AP
CVE-2021-27187,The Sovremennye Delovye Tekhnologii FX Aggregator terminal client 1 stores authentication credentials in cle
CVE-2021-27188,The Sovremennye Delovye Tekhnologii FX Aggregator terminal client 1 allows attackers to cause a denial of se
CVE-2021-27197,"DSUtility.dll in Pelco Digital Sentry Server before 7.19.67 has an arbitrary file write vulnerability. The
CVE-2021-27204,"Telegram before 7.4 (212543) Stable on macOS stores the local passcode in cleartext, leading to informatior
CVE-2021-27205,"Telegram before 7.4 (212543) Stable on macOS stores the local copy of self-destructed messages in a sandbo
CVE-2021-20188,"A flaw was found in podman before 1.7.0. File permissions for non-root users running in a privileged cont
CVE-2021-20335,"For MongoDB Ops Manager 4.2.X with multiple OM application servers, that have SSL turned on for their
```

JSON



```
[ ⊟
   { ⊟
      "title":"CVE-2019-16154",
      "content":"An improper neutralization of input during web page generation in FortiAuthenticator WEB UI 6.0.0 may allow an unauthenticate
      "date":"2020-01-07",
      "references":[ ⊟
         "[https://fortiguard.com/advisory/FG-IR-19-104]"
      ]
   },
   { ⊟
      "title":"CVE-2014-5209",
      "content":"An Information Disclosure vulnerability exists in NTP 4.2.7p25 private (mode 6/7) messages via a GET_RESTRICT control message
      "date":"2020-01-07",
      "references":[ ⊟
         "[https://support.f5.com/csp/article/K44942017, https://support.f5.com/csp/article/K44942017?utm_source=f5support&amp;utm_medium=RSS,
      ]
   },
   { ⊟
      "title":"CVE-2019-10776",
      "content":"In \"index.js\" file line 240, the run command executes the git command with a user controlled variable called remoteUrl. Thi
      "date":"2020-01-07",
      "references":[ ⊟
         "[https://snyk.io/vuln/SNYK-JS-GITDIFFAPPLY-540774,, https://github.com/kellyselden/git-diff-apply/commit/106d61d3ae723b4257c2a13e67b
      ]
   },
   { ⊟
      "title":"CVE-2019-14819",
      "content":"A flaw was found during the upgrade of an existing OpenShift Container Platform 3.x cluster. Using CRI-O, the dockergc servic
      "date":"2020-01-07",
      "references":[ ⊟
         "[https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2019-14819]"
      ]
   },
```

XML



ıs XML file does not appear to have any style information associated with it. The document tree is shown below.

```
<Vulnerabilities>
▼<CVE>
    <Title>CVE-2019-16154</Title>
    <Content>An improper neutralization of input during web page generation in FortiAuthenticator WEB UI 6.0.0 may allow an unauthenticated user to perform a
    scripting attack (XSS) via a parameter of the logon page.</Content>
    <Date>2020-01-07</Date>
  ▼<References>
      <URL>https://fortiguard.com/advisory/FG-IR-19-104</URL>
    </References>
  </CVE>
▼<CVE>
    <Title>CVE-2014-5209</Title>
    <Content>An Information Disclosure vulnerability exists in NTP 4.2.7p25 private (mode 6/7) messages via a GET_RESTRICT control message, which could let a
    user obtain sensitive information.</Content>
    <Date>2020-01-07</Date>
  ▼<References>
      <URL>https://support.f5.com/csp/article/K44942017</URL>
      <URL>https://support.f5.com/csp/article/K44942017?utm_source=f5support&amp;utm_medium=RSS</URL>
      <URL>https://exchange.xforce.ibmcloud.com/vulnerabilities/95841</URL>
    </References>
  </CVE>
▼<CVE>
    <Title>CVE-2019-10776</Title>
    <Content>In "index.js" file line 240, the run command executes the git command with a user controlled variable called remoteUrl. This affects git-diff-ap
    versions prior to 0.22.2.</Content>
    <Date>2020-01-07</Date>
  ▼<References>
      <URL>https://snyk.io/vuln/SNYK-JS-GITDIFFAPPLY-540774,</URL>
      <URL>https://github.com/kellyselden/git-diff-apply/commit/106d61d3ae723b4257c2a13e67b95eb40a27e0b5</URL>
    </References>
  </CVE>
▼<CVE>
    <Title>CVE-2019-14819</Title>
    <Content>A flaw was found during the upgrade of an existing OpenShift Container Platform 3.x cluster. Using CRI-O, the dockergc service account is assign
    current namespace of the user performing the upgrade. This flaw can allow an unprivileged user to escalate their privileges to those allowed by the privi
    Context Constraints.</Content>
    <Date>2020-01-07</Date>
  ▾<References>
```