

2023-07-13 16:08:31,385 ERROR pid=7210 tid=MainThread file=base_modinput.py:log_error:309 | Error in input_module_trellix_edr_input.get_threats() - line 127 : HTTPSConnectionPool(host='api.soc.us-east-1.mcafee.com', port=443): Max retries exceeded with url: /ft/api/v2/ft/threats?sort=-lastDetected&filter=%7B%22severities%22:%20%5B%22s0%22,%20%22s1%22,%20%22s2%22,%20%22s3%22,%20%22s4%22,%20%22s5%22%5D,%20%22scoreRange%22:%20%5B30%5D%7D&from=1686690509938&limit=10000&skip=0 (Caused by SSLError(SSLCertVerificationError(1, '[SSL: CERTIFICATE_VERIFY_FAILED] certificate verify failed: unable to get local issuer certificate (_ssl.c:1106)')))

2023-07-13 16:08:31,427 ERROR pid=7210 tid=MainThread file=base_modinput.py:log_error:309 | Get error when collecting events.

Traceback (most recent call last):

```
File "/opt/splunk/etc/apps/TA-trellix-edr-detections/bin/ta_trellix_edr_detections/aob_py3/urllib3/connectionpool.py", line 710, in urlopen
    chunked=chunked,
File "/opt/splunk/etc/apps/TA-trellix-edr-detections/bin/ta_trellix_edr_detections/aob_py3/urllib3/connectionpool.py", line 386, in _make_request
    self._validate_conn(conn)
File "/opt/splunk/etc/apps/TA-trellix-edr-detections/bin/ta_trellix_edr_detections/aob_py3/urllib3/connectionpool.py", line 1040, in _validate_conn
    conn.connect()
File "/opt/splunk/etc/apps/TA-trellix-edr-detections/bin/ta_trellix_edr_detections/aob_py3/urllib3/connection.py", line 426, in connect
    tls_in_tls=tls_in_tls,
File "/opt/splunk/etc/apps/TA-trellix-edr-detections/bin/ta_trellix_edr_detections/aob_py3/urllib3/util/ssl_.py", line 450, in ssl_wrap_socket
    sock, context, tls_in_tls, server_hostname=server_hostname
File "/opt/splunk/etc/apps/TA-trellix-edr-detections/bin/ta_trellix_edr_detections/aob_py3/urllib3/util/ssl_.py", line 493, in _ssl_wrap_socket_impl
    return ssl_context.wrap_socket(sock, server_hostname=server_hostname)
File "/opt/splunk/lib/python3.7/ssl.py", line 428, in wrap_socket
    session=session
File "/opt/splunk/lib/python3.7/ssl.py", line 878, in _create
    self.do_handshake()
File "/opt/splunk/lib/python3.7/ssl.py", line 1147, in do_handshake
    self._sslobj.do_handshake()
ssl.SSLCertVerificationError: [SSL: CERTIFICATE_VERIFY_FAILED] certificate verify failed: unable to get local issuer certificate (_ssl.c:1106)
```

During handling of the above exception, another exception occurred:

Traceback (most recent call last):

```
File "/opt/splunk/etc/apps/TA-trellix-edr-detections/bin/ta_trellix_edr_detections/aob_py3/requests/adapters.py", line 449, in send
    timeout=timeout
File "/opt/splunk/etc/apps/TA-trellix-edr-detections/bin/ta_trellix_edr_detections/aob_py3/urllib3/connectionpool.py", line 786, in urlopen
    method, url, error=e, _pool=self, _stacktrace=sys.exc_info()[2]
File "/opt/splunk/etc/apps/TA-trellix-edr-detections/bin/ta_trellix_edr_detections/aob_py3/urllib3/util/retry.py", line 592, in increment
    raise MaxRetryError(_pool, url, error or ResponseError(cause))
urllib3.exceptions.MaxRetryError: HTTPSConnectionPool(host='api.soc.us-east-1.mcafee.com', port=443): Max retries exceeded with url: /ft/api/v2/ft/threats?sort=-lastDetected&filter=%7B%22severities%22:%20%5B%22s0%22,%20%22s1%22,%20%22s2%22,%20%22s3%22,%20%22s4%22,%20%22s5%22%5D,%20%22scoreRange%22:%20%5B30%5D%7D&from=1686690509938&limit=10000&skip=0 (Caused by SSLError(SSLCertVerificationError(1, '[SSL: CERTIFICATE_VERIFY_FAILED] certificate verify failed: unable to get local issuer certificate (_ssl.c:1106)')))
```

During handling of the above exception, another exception occurred:

Traceback (most recent call last):

```
File "/opt/splunk/etc/apps/TA-trellix-edr-detections/bin/ta_trellix_edr_detections/aob_py3/modinput_wrapper/base_modinput.py", line 128, in stream_events
    self.collect_events(ew)
File "/opt/splunk/etc/apps/TA-trellix-edr-detections/bin/trellix_edr_input.py", line 76, in collect_events
    input_module.collect_events(self, ew)
File "/opt/splunk/etc/apps/TA-trellix-edr-detections/bin/input_module_trellix_edr_input.py", line 76, in collect_events
    get_threats(helper, session, base_url, ldttime, epoch_pull, limit, ew)
File "/opt/splunk/etc/apps/TA-trellix-edr-detections/bin/input_module_trellix_edr_input.py", line 127, in get_threats
    .format(base_url, json.dumps(filter), epoch_pull, limit, skip))
File "/opt/splunk/etc/apps/TA-trellix-edr-detections/bin/ta_trellix_edr_detections/aob_py3/requests/sessions.py", line 555, in get
    return self.request('GET', url, **kwargs)
File "/opt/splunk/etc/apps/TA-trellix-edr-detections/bin/ta_trellix_edr_detections/aob_py3/requests/sessions.py", line 542, in request
    resp = self.send(prepare_request(self, url, **kwargs))
File "/opt/splunk/etc/apps/TA-trellix-edr-detections/bin/ta_trellix_edr_detections/aob_py3/requests/sessions.py", line 655, in send
    r = adapter.send(request, **kwargs)
File "/opt/splunk/etc/apps/TA-trellix-edr-detections/bin/ta_trellix_edr_detections/aob_py3/requests/adapters.py", line 514, in send
    raise SSLError(e, request=request)
requests.exceptions.SSLError: HTTPSConnectionPool(host='api.soc.us-east-1.mcafee.com', port=443): Max retries exceeded with url: /ft/api/v2/ft/threats?sort=-lastDetected&filter=%7B%22severities%22:%20%5B%22s0%22,%20%22s1%22,%20%22s2%22,%20%22s3%22,%20%22s4%22,%20%22s5%22%5D,%20%22scoreRange%22:%20%5B30%5D%7D&from=1686690509938&limit=10000&skip=0 (Caused by SSLError(SSLCertVerificationError(1, '[SSL: CERTIFICATE_VERIFY_FAILED] certificate verify failed: unable to get local issuer certificate (_ssl.c:1106)'))))
```