Talos Vulnerability Report

TALOS-2020-1106

Aveva eDNA Enterprise data historian CHaD.asmx multiple SQL injection vulnerabilities

SEPTEMBER 23, 2020

CVE NUMBER

CVE-2020-13501,CVE-2020-13499,CVE-2020-13500

SUMMARY

Multiple SQL injection vulnerabilities exists in the CHaD.asmx web service functionality of eDNA Enterprise Data Historian 3.0.1.2/7.5.4989.33053. Specially crafted SOAP web requests can cause SQL injections resulting in data compromise. An attacker can send unauthenticated HTTP requests to trigger these vulnerabilities.

CONFIRMED VULNERABLE VERSIONS

The versions below were either tested or verified to be vulnerable by Talos or confirmed to be vulnerable by the vendor.

Aveva eDNA Enterprise Data Historian 3.0.1.2/7.5.4989.33053

PRODUCT URLS

eDNA Enterprise Data Historian - https://sw.aveva.com/asset-performance/industrial-information-management/enterprise-data-management

CVSSV3 SCORE

9.8 - CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

CWE

CWE-89 - Improper Neutralization of Special Elements used in an SQL Command (‘SQL Injection’)

DETAILS

.eDNA Enterprise Data Historian is highly scalable software platform that efficiently archives and quickly retrieves time-series data in business and operational environments.

Multiple SQL injection vulnerabilities exist within the web service as an unauthenticated user. A successful attack could allow an unauthenticated attacker to access information such as usernames and password hashes that are stored in the database.

CVE-2020-13499 - Parameter InstancePath

Parameter InstancePath in CHaD.asmx is vulnerable to unauthenticated SQL injection attacks::

```
POST /webservice/CHaD.asmx HTTP/1.1
Accept-Encoding: gzip,deflate
Content-Type: application/soap+xml;charset=UTF-8;action="http://instepsoftware.com/webservices/FindCHaDInstances"
User-Agent: agent
Host: [IP]
Content-Length: 509

<soap:Envelope xmlns:soap="http://www.w3.org/2003/05/soap-envelope" xmlns:web="http://instepsoftware.com/webservices">
  <soap:Header/>
  <soap:Body>
     <web:FindCHaDInstances>
        <web:InstancePath>(SQL INJECTION)</web:InstancePath>
        <web:InstanceName>bb</web:InstanceName>
        <web:ClassName>aa</web:ClassName>
     </web:FindCHaDInstances>
  </soap:Body>
</soap:Envelope>
```

CVE-2020-13500 - Parameter ClassName

Parameter ClassName in CHaD.asmx is vulnerable to unauthenticated SQL injection attacks::

```
POST /webservice/CHaD.asmx HTTP/1.1
Accept-Encoding: gzip,deflate
Content-Type: application/soap+xml;charset=UTF-8;action="http://instepsoftware.com/webservices/FindCHaDInstances"
User-Agent: agent
Host: [IP]
Content-Length: 509

<soap:Envelope xmlns:soap="http://www.w3.org/2003/05/soap-envelope" xmlns:web="http://instepsoftware.com/webservices">
   <soap:Header/>
   <soap:Body>
     <web:FindCHaDInstances>
        <web:InstancePath>aaa</web:InstancePath>
        <web:InstanceName>bbb</web:InstanceName>
        <web:ClassName>(SQL INJECTION)</web:ClassName>
     </web:FindCHaDInstances>
  </soap:Body>
</soap:Envelope>
```

CVE-2020-13501 - Parameter InstanceName

Parameter InstanceName in CHaD.asmx is vulnerable to unauthenticated SQL injection attacks::

```
POST /webservice/CHaD.asmx HTTP/1.1
Accept-Encoding: gzip,deflate
Content-Type: application/soap+xml;charset=UTF-8;action="http://instepsoftware.com/webservices/FindCHaDInstances"
User-Agent: agent
Host: [IP]
Content-Length: 509

<soap:Envelope xmlns:soap="http://www.w3.org/2003/05/soap-envelope" xmlns:web="http://instepsoftware.com/webservices">
  <soap:Header/>
  <soap:Body>
     <web:FindCHaDInstances>
        <web:InstancePath>aaa</web:InstancePath>
        <web:InstanceName>(SQL INJECTION)</web:InstanceName>
        <web:ClassName>bbb</web:ClassName>
     </web:FindCHaDInstances>
  </soap:Body>
</soap:Envelope>
```

TIMELINE

2020-07-10 - Vendor disclosure

2020-08-10 - Vendor provided patch for Talos to test

2020-08-18 - Talos confirmed fix/patch

2020-08-27 - Public disclosure release

CREDIT

Discovered by Yuri Kramarz of Cisco Talos.

VULNERABILITY REPORTS

PREVIOUS REPORT TALOS-2020-1084

NEXT REPORT TALOS-2020-1129