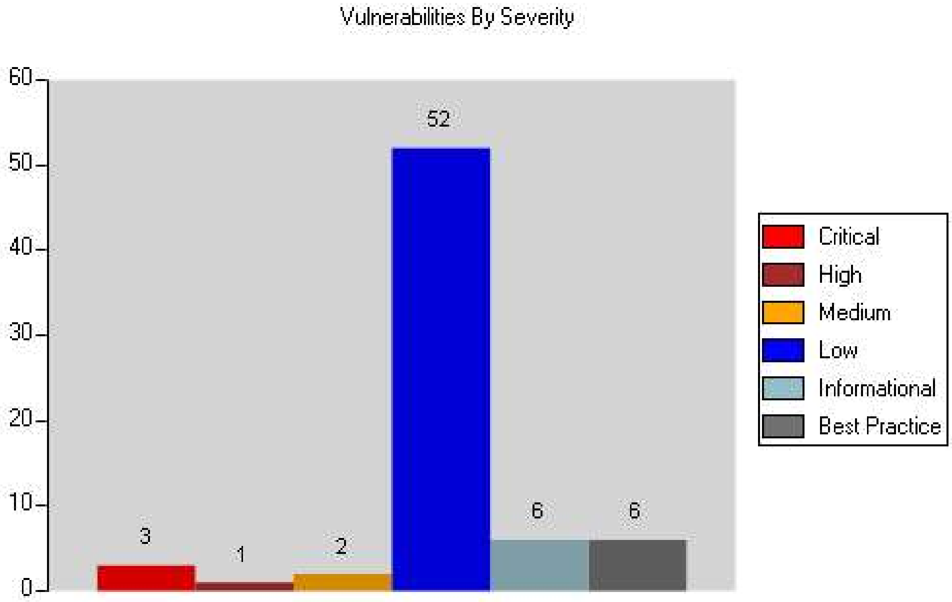
Micro Focus WebInspect

Vulnerability (Legacy)

Web Application Assessment Report

Scan Name:	Market Place-Delta - Manual		
Policy:	OWASP Top 10 2017 - (OWASP 2017)	**Crawl Sessions:**	35
Scan Date:	3/12/2019 5:23:23 PM	**Vulnerabilities:**	58
Scan Version:	18.20.178.0	**Scan Duration:**	1 hour : 8 minutes
Scan Type:	Site	**Client:**	FF

Server: https://pit.deltadentalins.com:443



Critical

Insecure Transport: Weak SSL Cipher

Summary:

WebInspect has detected support for weak TLS/SSL ciphers on server **https://pit.deltadentalins.com:443/** .

The Transport Layer Security (TLS) and Secure Sockets Layer (SSL) protocols provide a mechanism to help protect authenticity, confidentiality and integrity of the data transmitted between a client and web server. The strength of this protection mechanism is determined by the authentication, encryption and hashing algorithms, collectively known as a cipher suite, chosen for the transmission of sensitive information over the TLS/SSL channel. Most Web servers support a range of such cipher suites of varying strengths. Using a weak cipher or an encryption key of insufficient length, for example, could allow an attacker to defeat the protection mechanism and steal or modify sensitive information.

If misconfigured, a web server could be manipulated into choosing weak cipher suites. Recommendations include updating the web server configuration to always choose the strongest ciphers for encryption.

Execution:

Each weak cipher was enumerated by establishing an SSL connection with the target host and specifying the cipher to test in the Client Hello message of the SSL handshake.

Implication:

A weak encryption scheme can be subjected to brute force attacks that have a reasonable chance of succeeding using current methods and resources. An attacker may be able to execute a man-in-the-middle attack which would allow them to intercept, monitor and tamper with sensitive data.

Fix:

Disable support for weak ciphers on the server. Weak ciphers are generally defined as:

- Any cipher with key length less than 128 bits
- Export-class cipher suites
- NULL ciphers
- Ciphers that support unauthenticated modes
- Ciphers assessed at security strenghts below 112 bits
- All RC4 ciphers
- All 64-bit block ciphers

The following ciphers supported by the server are weak and should be disabled:

- **TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (0x16)**
- **TLS_RSA_WITH_3DES_EDE_CBC_SHA (0xa)**
- **TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA (0xc012)**

The weak cipher list above also includes ciphers that enable conditions for SWEET32 cipher attacks. The vulnerability affects all 64-bit block ciphers such as 3DES and Blowfish. The vulnerability is independent of the number of keys and/or the key length used in the cipher. It could allow attackers to obtain cleartext data from long-lived encrypted sessions. The vulnerability is identified by CVE-2016-2183 and CVE-2016-6329.

The following 64-bit block ciphers should be removed from the target server configuration to prevent SWEET32 attacks:

- **TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (0x16)**
- **TLS_RSA_WITH_3DES_EDE_CBC_SHA (0xa)**
- **TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA (0xc012)**

- For Apache, modify the following lines in httpd.conf or ssl.conf:

- SSLCipherSuite ALL:!aNULL:!ADH:!eNULL:!LOW:!EXP:!NULL:!RC4:!RC2:!DES:!3DES+HIGH:+MEDIUM

- For IIS, please refer to Microsoft Knowledge Base Articles:

- Article ID: 187498
- Article ID: 245030 and
- Security Guidance for IIS
- Article ID: 2868725

- For other servers, please refer to vendor specific documentation.

The following ciphers supported by the server should provide adequate protection and may be left enabled:

- **TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39)**
- **TLS_RSA_WITH_AES_256_CBC_SHA (0x35)**
- **TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x33)**
- **TLS_RSA_WITH_AES_128_CBC_SHA (0x2f)**
- **TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA (0x45)**
- **TLS_RSA_WITH_CAMELLIA_128_CBC_SHA (0x41)**
- **TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA (0x88)**
- **TLS_RSA_WITH_CAMELLIA_256_CBC_SHA (0x84)**

- **TLS_RSA_WITH_AES_256_CBC_SHA256 (0x3d)**
- **TLS_RSA_WITH_AES_128_CBC_SHA256 (0x3c)**
- **TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (0x6b)**
- **TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (0x67)**
- **TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (0x9f)**
- **TLS_RSA_WITH_AES_256_GCM_SHA384 (0x9d)**
- **TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (0x9e)**
- **TLS_RSA_WITH_AES_128_GCM_SHA256 (0x9c)**
- **TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)**
- **TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028)**
- **TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)**
- **TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)**
- **TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027)**
- **TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)**

Reference:

OWASP:
Transport Layer Protection Cheat Sheet

PCI Security Standards Council:
PCI DSS v3.1

CVE
CVE-2013-2566
CVE-2016-2183
CVE-2016-6329

NIST
NIST Special Publication 800-131A

Microsoft:
Knowledge Base Article ID: 2868725
Knowledge Base Article ID: 187498
Knowledge Base Article ID: 245030
Security Guidance for IIS

Apache:
SSL/TLS Strong Encryption: FAQ

RC4:
New RC4 Attack

ACM CCS '16
On the Practical (In-)Security of 64-bit Block Ciphers: Collision Attacks on HTTP over TLS and OpenVPN

Attack Request:

```
GET /shopping/delta/get-a-quote?issuerCode=DELTA HTTP/1.1
Accept: */*
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64; rv:30.0) Gecko/20100101 Firefox/30.0
Accept-Encoding: gzip, deflate
Host: pit.deltadentalins.com
Connection: Keep-Alive
Pragma: no-cache
Cookie: _ga=GA1.2.1222917316.1517435630; AMCV_E9D70FA75B3A18E80A495C49%40AdobeOrg=1994364360%
7CMCIDTS%7C17967%7CMCMID%7C22137510049759883710112622098244936722%7CMCAAMLH-1552928317%7C9%
7CMCAAMB-1552928317%7CRKhpRz8krg2tLO6pguXWp5olkAcUniQYPHaMWWgdJ3xzPWQmdj0y%7CMCOPTOUT-
1552330717s%7CNONE%7CvVersion%7C3.4.0%7CMCAID%7CNONE%7CMCSYNCSOP%7C411-17946;
```

```
_gid=GA1.2.1396295264.1552431132; _gcl_au=1.1.404074092.1552323525;
_fbp=fb.1.1552323526191.52071667;CustomCookie=WebInspect141622ZXE000CE7833EE4CBCB1B0690CD295CDC0YC8A5
```

Attack Response:

```
HTTP/1.1 200 OK
Date: Wed, 13 Mar 2019 00:23:29 GMT
X-Frame-Options: SAMEORIGIN
Content-Type: text/html; charset=utf-8
Content-Length: 16129
ETag: W/"3f01-Sn+DneAOjpxnqwVNVujOl+91Y3U"
Set-Cookie: connect.sid=s%3A2elaWPMp1jpy7vDuK3ggeUpv3kIzZWuL.lbXc8mr31%2FQJ987wrTAX8m2K%
2FKYWnisjECietMsNrjw; Path=/; HttpOnly; Secure
Set-Cookie: ADRUM_BT=R:0|g:070481de-7715-4e9f-bd7f-29b2acf368e95648|s:f|n:PIT_948e56b2-cdee-4f42-bf8d-
46318aebf03f; Path=/; Expires=Wed, 13 Mar 2019 00:23:59 GMT; Secure
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Set-Cookie: BIGipServer~UNIX_Systems~PIT_DDINS-SSL=2711618826.64288.0000; path=/; Httponly; Secure

<!DOCTYPE html>
<html lang="en">
<head>
  <meta charset="UTF-8">
  <meta name="viewport" content="width=device-width, initial-scale=1.0">
  <meta http-equiv="X-UA-Compatible" content="IE=edge" />
  <title>Get A Quote</title>

  <!-- Page-hiding snippet (recommended)  -->
  <style>.async-hide { opacity: 0 !important} </style>
  <script>(function(a,s,y,n,c,h,i,d,e){s.className+=' '+y;h.start=1*new Date;
    h.end=i=function(){s.className=s.className.replace(RegExp(' ?'+y),")};
    (a[n]=a[n]||[]).hide=h;setTimeout(function(){i();h.end=null},c);h.timeout=c;
  })(window,document.documentElement,'async-hide','dataLayer',4000,
      {'GTM-NPRVDTC':true});</script>
  <!-- Modified Analytics tracking code with Optimize plugin -->
  <script type="text/javascript">
    (function(i, s, o, g, r, a, m) {
      i['GoogleAnalyticsObject'] = r;
      i[r] = i[r] || function() {
            (i[r].q = i[r].q || []).push(arguments)
          }, i[r].l = 1 * new Date();
      a = s.createElement(o), m = s.getElementsByTagName(o)[0];
      a.async = 1;
      a.src = g;
      m.parentNode.insertBefore(a, m)
    })(window, document, 'script', '//www.google-analytics.com/analytics.js', 'ga');
    ga('create', 'UA-9398012-1', 'auto');
    ga('require', 'GTM-NPRVDTC', 'auto');
    var dnt= navigator.doNotTrack || window.doNotTrack || window.msDoNotTrack;
    ga('set', 'dimension9', dnt);
    ga('send', 'pageview');
  </script>

    <script type="text/javascript" src="https://maps.googleapis.com/maps/api/js?client=gme-
deltadentalofcalifornia&libraries=places"></script>
    <script type="text/javascript" src="/shopping/js/jquery-8101d596b2.js"></script>

  <script>window['adrum-start-time'] = new Date().getTime();</script>
  <script type="text/javascript" src="/shopping/js/html5shiv-40bd440d29.min.js" async></script>


    <link rel="stylesheet" type="text/css" href="/shopping/styles/style-67c2fc579a.css">


  <link rel="stylesheet" type="text/css" href="//cloud.typography.com/6549574/670548/css/fonts.css" />
</head>
<body>
<!-- MAIN CONTENT -->
        <header class="shopping-header-title">

                                            <a class="back-arrow-link" id="shoppingBack"
href="https://pit.deltadentalins.com/"><i class="icon  icon-back-arrow-shopping" aria-label="shopping back arrow icon"
><span class="visually-hidden">back to previous page</span></i>
<span class="visually-hidden">back to previous page</span></a>
```

```
                                        <div class="main-content">
                                                <h1 class="shopping-header-content">
                                                        Get a Quote
                                                </h1>
                                        </div>
                                        </header>


    <main role="main" class="main-content container page-control get-a-quote">
      <div class="main-container-inner">
        <div class="top-heading-section">
            <div class="error-container global-margin">
            </div>
          <div class="summary grey-text">
            We need a little more information to give you a quote.
          </div>
        </div>
        <form id="get_a_quote" action="/shopping/delta/get-a-quote" method="post">
          <input type="hidden" id="jsEnabled" name="jsEnabled" value="false" />
              <label for="zip"   >What’s your ZIP code?</label>
              <input id="zip"  class="form-input quote_address_zip zip"  type="text" name="zip"  placeholder="ZIP code"       />

              <div class="inline-error-container"

    ...TRUNCATED...
```

File Names:

- https://pit.deltadentalins.com:443/shopping/delta/get-a-quote?issuerCode=DELTA

Critical

Query String Injection: MongoDB

Summary:

MongoDB is a type of NoSQL database that supports JSON-oriented document storage format. The MongoDB PHP driver is vulnerable to a request injection attack since PHP allows objects to be passed in via HTTP GET and HTTP POST requests and doesn’t inherently sanitize input parameters. A simple variable can be easily converted into array object by passing it as an array reference. An instance of this vulnerability was discovered in the following URL: https://pit.deltadentalins.com:443/enroll/delta/personal-info.

Implication:

This vulnerability can be used to bypass authentication and obtain unauthorized access to information stored in the MongoDB backend database.

Fix:

All variables in /enroll/delta/ that access request parameters, either through HTTP POST or HTTP GET, should be strongly typed.
e.g.

```
username = (string)$_GET['username'];
password = (string)$_GET['password'];
```

Reference:

http://us.php.net/manual/en/mongo.security.php

Attack Request:

```
POST /enroll/delta/personal-info HTTP/1.1
Accept: */*
Referer: https://pit.deltadentalins.com/shopping/delta/plan-options/9801677?issuerCode=DELTA
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64; rv:30.0) Gecko/20100101 Firefox/30.0
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip, deflate
Host: pit.deltadentalins.com
Content-Length: 267
Cache-Control: no-cache
Pragma: no-cache
Connection: Keep-Alive
X-WIPP: AscVersion=18.20.178.0
X-Scan-Memo: Category="Audit.Attack"; SID="FD8518C2DF04BF39D88A194B1D702290";
```

```
PSID="4920DEA7FFC96CDF6C75400C1A028D73"; SessionType="AuditAttack"; CrawlType="None"; AttackType="Other";
OriginatingEngineID="a9e4d941-5d29-4cef-8ce0-24ee80bc86ba"; AttackSequence="0";
AttackParamDesc="coverageStartDate"; AttackParamIndex="10"; AttackParamSubIndex="0"; CheckId="11298";
Engine="Mongo+DB+Request+Injection+Attack"; SmartMode="ServerSpecificOnly"; ThreadId="295";
ThreadType="AuditorStateRequestor";
X-RequestManager-Memo: RequestorThreadIndex="0"; sid="470"; smi="0"; sc="1"; ID="ace59c04-59ec-4001-abe5-
fde4f8bf5c37";
X-Request-Memo: ID="c3ffe1a6-2443-408f-a968-8acfb970cbea"; sc="1"; ThreadId="295";
Cookie: ADRUM_BT=R:83|g:6f065e8e-3eec-49ec-bc79-771467447e5a537|n:PIT_948e56b2-cdee-4f42-bf8d-46318aebf03f;
connect.sid=s%3AL_7qxbMgbNFHlwX8JqoPmedNSnSMwlfG.tCSuwthT3%2Bf5GN5rAuAPK6U2Ko51X05rRnP%2BoHEO9dE;
BIGipServer~UNIX_Systems~PIT_DDINS-SSL=2711618826.64288.0000; ADRUM=s=1552437757258&r=https%3A%2F%
2Fpit.deltadentalins.com%2Fshopping%2Fdelta%2Fplan-options%3F-
1555445888;CustomCookie=WebInspect141622ZXE000CE7833EE4CBCB1B0690CD295CDC0YC8A5;ADRUM=s=155243775725
8&r=https%3A%2F%2Fpit.deltadentalins.com%2Fshopping%2Fdelta%2Fplan-options%3F-
1555445888;ADRUM=s=1552437757258&r=https%3A%2F%2Fpit.deltadentalins.com%2Fshopping%2Fdelta%2Fplan-
options%3F-1555445888

planType=PPO&planCode=Basic00001&planId=9801677&planName=Delta+Dental+PPO+Individual+-
+Basic+Plan&annualCost=33.91&enrollmentFee=10&planState=CA&planZip=95630&coverageType=Self&issuerCode=DELTA
&coverageStartDate[$ne]=WIMongoDBAttack&noOfCovered=1&a_dob=02%2F02%2F1981
```

Attack Response:

```
HTTP/1.1 503 Service Temporarily Unavailable
Date: Wed, 13 Mar 2019 01:30:56 GMT
X-Frame-Options: SAMEORIGIN
Content-Length: 323
X-Cnection: close
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>503 Service Temporarily Unavailable</title>
</head><body>
<h1>Service Temporarily Unavailable</h1>
<p>The server is temporarily unable to service your
request due to maintenance downtime or capacity
problems. Please try again later.</p>
</body></html>
```

File Names:

- https://pit.deltadentalins.com:443/enroll/delta/personal-info

Critical

Insecure Transport: Insufficient Diffie Hellman Strength

Summary:

Using Diffie Hellman group with prime (*p*or small prime) of size 1024-bit or less, leaves the server vulnerable to man-in-the middle attack (MitM).

Diffie-Hellman key exchange algorithm uses fixed primes as a base for computing the secret key used to secure the communication channel. The size of the small prime *p*deployed dictates the security level of the generated key. This in turn defines the effective security provided by the Diffie-Helman key exchange algorithm. Research indicates that Diffie-Hellman group using prime size of 1024-bit provides only about 77-80 bits of security. Communication channels that are secured using this key are vulnerable to man-in-the-middle attack. All anonymous, ephermeral and fixed Diffie-Hellman key exchange algorithms **except** for Elliptical-Curve Diffie-Hellman (ECDHE) key exchange are vulnerable to this attack.

WebInspect has detected the target server using Diffie-Hellman small prime *p*of size **1024** bits in ciphersuite: **TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (0x16)**.

The server may thus be vulnerable to eavesdropping and/or man-in-the-middle attacks.

Implication:

Using Diffie Hellman group with prime (*p*or small prime) of size 1024-bit or less, leaves the server vulnerable to man-in-the middle attack (MitM).

Fix:

- Disable the use of export cipher suites.
- Ensure that the servers use strong Diffie Hellman group with prime of size 2048-bit or more.
- Reject any connections that accept Diffie-Hellman primes smaller than 1024-bit.
- Deploy Elliptic-Curve Diffie-Hellman (ECDHE) key exchange.

Reference:

[Imperfect Forward Secrecy: How Diffie-Hellman Fails in Practice]

Attack Request:

```
GET /shopping/delta/get-a-quote?issuerCode=DELTA HTTP/1.1
Accept: */*
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64; rv:30.0) Gecko/20100101 Firefox/30.0
Accept-Encoding: gzip, deflate
Host: pit.deltadentalins.com
Connection: Keep-Alive
Pragma: no-cache
Cookie: _ga=GA1.2.1222917316.1517435630; AMCV_E9D70FA75B3A18E80A495C49%40AdobeOrg=1994364360%
7CMCIDTS%7C17967%7CMCMID%7C22137510049759883710112622098244936722%7CMCAAMLH-1552928317%7C9%
7CMCAAMB-1552928317%7CRKhpRz8krg2tLO6pguXWp5olkAcUniQYPHaMWWgdJ3xzPWQmdj0y%7CMCOPTOUT-
1552330717s%7CNONE%7CvVersion%7C3.4.0%7CMCAID%7CNONE%7CMCSYNCSOP%7C411-17946;
_gid=GA1.2.1396295264.1552431132; _gcl_au=1.1.404074092.1552323525;
_fbp=fb.1.1552323526191.52071667;CustomCookie=WebInspect141622ZXE000CE7833EE4CBCB1B0690CD295CDC0YC8A5
```

Attack Response:

```
HTTP/1.1 200 OK
Date: Wed, 13 Mar 2019 00:23:29 GMT
X-Frame-Options: SAMEORIGIN
Content-Type: text/html; charset=utf-8
Content-Length: 16129
ETag: W/"3f01-Sn+DneAOjpxnqwVNVujOl+91Y3U"
Set-Cookie: connect.sid=s%3A2elaWPMp1jpy7vDuK3ggeUpv3kIzZWuL.lbXc8mr31%2FQJ987wrTAX8m2K%
2FKYWnisjECietMsNrjw; Path=/; HttpOnly; Secure
Set-Cookie: ADRUM_BT=R:0|g:070481de-7715-4e9f-bd7f-29b2acf368e95648|s:f|n:PIT_948e56b2-cdee-4f42-bf8d-
46318aebf03f; Path=/; Expires=Wed, 13 Mar 2019 00:23:59 GMT; Secure
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Set-Cookie: BIGipServer~UNIX_Systems~PIT_DDINS-SSL=2711618826.64288.0000; path=/; Httponly; Secure

<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <meta http-equiv="X-UA-Compatible" content="IE=edge" />
    <title>Get A Quote</title>

    <!-- Page-hiding snippet (recommended)  -->
    <style>.async-hide { opacity: 0 !important} </style>
    <script>(function(a,s,y,n,c,h,i,d,e){s.className+=' '+y;h.start=1*new Date;
        h.end=i=function(){s.className=s.className.replace(RegExp(' ?'+y),'')};
        (a[n]=a[n]||[]).hide=h;setTimeout(function(){i();h.end=null},c);h.timeout=c;
    })(window,document.documentElement,'async-hide','dataLayer',4000,
            {'GTM-NPRVDTC':true});</script>
    <!-- Modified Analytics tracking code with Optimize plugin -->
    <script type="text/javascript">
        (function(i, s, o, g, r, a, m) {
            i['GoogleAnalyticsObject'] = r;
            i[r] = i[r] || function() {
                        (i[r].q = i[r].q || []).push(arguments)
                    }, i[r].l = 1 * new Date();
            a = s.createElement(o), m = s.getElementsByTagName(o)[0];
            a.async = 1;
            a.src = g;
            m.parentNode.insertBefore(a, m)
        })(window, document, 'script', '//www.google-analytics.com/analytics.js', 'ga');
        ga('create', 'UA-9398012-1', 'auto');
        ga('require', 'GTM-NPRVDTC', 'auto');
        var dnt= navigator.doNotTrack || window.doNotTrack || window.msDoNotTrack;
        ga('set', 'dimension9', dnt);
        ga('send', 'pageview');
    </script>

        <script type="text/javascript" src="https://maps.googleapis.com/maps/api/js?client=gme-
deltadentalofcalifornia&libraries=places"></script>
        <script type="text/javascript" src="/shopping/js/jquery-8101d596b2.js"></script>
    <script>window['adrum-start-time'] = new Date().getTime();</script>
    <script type="text/javascript" src="/shopping/js/html5shiv-40bd440d29.min.js" async></script>


        <link rel="stylesheet" type="text/css" href="/shopping/styles/style-67c2fc579a.css">


    <link rel="stylesheet" type="text/css" href="//cloud.typography.com/6549574/670548/css/fonts.css" />
</head>
<body>
<!-- MAIN CONTENT -->
               <header class="shopping-header-title">

                                                  <a class="back-arrow-link" id="shoppingBack"
href="https://pit.deltadentalins.com/"><i class="icon  icon-back-arrow-shopping" aria-label="shopping back arrow icon"
><span class="visually-hidden">back to previous page</span></i>
<span class="visually-hidden">back to previous page</span></a>

                                     <div class="main-content">
                                                  <h1 class="shopping-header-content">
                                                               Get a Quote
                                                  </h1>
                                     </div>
                                     </header>


<main role="main" class="main-content container page-control get-a-quote">
  <div class="main-container-inner">
    <div class="top-heading-section">
        <div class="error-container global-margin">
        </div>
      <div class="summary grey-text">
        We need a little more information to give you a quote.
      </div>
    </div>
    <form id="get_a_quote" action="/shopping/delta/get-a-quote" method="post">
      <input type="hidden" id="jsEnabled" name="jsEnabled" value="false" />
          <label for="zip"    >What’s your ZIP code?</label>
          <input id="zip"  class="form-input quote_address_zip zip"  type="text" name="zip"  placeholder="ZIP code"       />

          <div class="inline-error-container"

...TRUNCATED...
```

File Names:

- https://pit.deltadentalins.com:443/shopping/delta/get-a-quote?issuerCode=DELTA

High

Insecure Transport: Weak SSL Protocol

Summary:

The Transport Layer Security (TLS) protocol provides a protection mechanism to better protect authenticity, confidentiality and integrity of the data transmitted between a client and a web server. The TLS protocol has undergone various revisions resulting in periodic version updates. Each revision tries to address security weakness in prior versions and incorporate support for the latest in security measures. It is strongly recommended to use the latest version of the available protocol, whenever possible.

TLS 1.0 is considered insecure as it lacks support for strong ciphersuites and is known to be plagued by several known vulnerabilities. It either uses RC4 cipher, which is prone to bias attacks or uses Cipher Block Chaining (CBC) mode cipher, which enables condition for POODLE (Padding Oracle On Downgraded Legacy Encryption) attacks.

NIST Special Publication 800-52 Revision 1 no longer considers TLS 1.0 as strong cryptography. TLS 1.0 is also no longer in compliance with PCI DSS v3.1 requirements. PCI does not consider TLS 1.0 to be adequate to protect cardholder data and has deprecated its use starting June 2016.
Update: PCI DSS has extended deadline for migration to TLS1.1 or above to June 30, 2018. However, an early migration is recommended to ensure security of your data and applications.

WebInspect has detected conditions that could enable POODLE on the target server. The vulnerability is implementation dependent. It affects connections using certain TLS implementations that don't properly check the structure of the padding used in TLS packets. This could allow sensitive data transmitted on TLS connection to be leaked to a malicious user. The attack is identified by CVE-2014-8730.
Use of insecure protocol versions will weaken the strength of the transport protection and could allow an attacker to compromise, steal or modify sensitive information. Configuring the web server to use the most secure protocol, TLS 1.1 or TLS 1.2 is highly recommended.

Implication:

Use of a weak protocol such as TLS 1.0 leaves the connection vulnerable to man-in-the-middle attacks. This would allow the attacker to read and modify data on a secure TLS connection, thus compromising user security and privacy. Its use would also limit the use of strong cipher suites that help protect data integrity and confidentiality.

Fix:

Disable support for the TLS 1.0 protocol on the server. Both NIST 800-52 and PCI DSS v3.1 strongly recommend upgrade to the latest version of TLS available, TLS 1.2. Or, at a minimum an upgrade to TLS 1.1.

- For Apache, modify the following lines in the server configuration

- SSLProtocol ALL –SSLv2 -SSLv3 -TLSv1

- For Nginx, modify the following lines in server configuration:

- ssl_protocols TLSv1.1 TLSv1.2;

- For IIS, please refer to Microsoft Knowledge Base Articles:

- https://technet.microsoft.com/library/security/3009008

- For other servers, please refer to vendor specific documentation.

Please Note: Not all implementations of TLS are affected by POODLE. Please ensure the TLS implementation in use on the target server is not vulnerable to POODLE. Remove CBC mode ciphers to prevent the POODLE attack if applicable.

Reference:

OWASP:
Transport Layer Protection Cheat Sheet

NIST:
NIST SP 800-52 Revision 1

PCI Security Standards Council:
PCI DSS v3.1
Migrating from SSL and Early TLS
PCI SSC FAQ on impending revisions to PCI DSS, PA-DSS to address SSL protocol vulnerability

Microsoft:
Knowledge Base Article ID: 187498
Knowledge Base Article ID: 245030
Security Guidance for IIS

Apache:
SSL/TLS Strong Encryption: FAQ

CVE-2014-8730
CVE-2014-8730

POODLE Vulnerability Expands Beyond SSLv3 to TLS 1.0 and 1.1
https://www.globalsign.com/en/blog/poodle-vulnerability-expands-beyond-sslv3-to-tls/

TLS Fallback Signaling Cipher Suite Value (SCSV) for Preventing Protocol Downgrade Attacks
https://tools.ietf.org/html/draft-ietf-tls-downgrade-scsv-00l

Attack Request:

```
GET /shopping/delta/get-a-quote?issuerCode=DELTA HTTP/1.1
Accept: */*
```

```
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64; rv:30.0) Gecko/20100101 Firefox/30.0
Accept-Encoding: gzip, deflate
Host: pit.deltadentalins.com
Connection: Keep-Alive
Pragma: no-cache
Cookie: _ga=GA1.2.1222917316.1517435630; AMCV_E9D70FA75B3A18E80A495C49%40AdobeOrg=1994364360%
7CMCIDTS%7C17967%7CMCMID%7C22137510049759883710112622098244936722%7CMCAAMLH-1552928317%7C9%
7CMCAAMB-1552928317%7CRKhpRz8krg2tLO6pguXWp5olkAcUniQYPHaMWWgdJ3xzPWQmdj0y%7CMCOPTOUT-
1552330717s%7CNONE%7CvVersion%7C3.4.0%7CMCAID%7CNONE%7CMCSYNCSOP%7C411-17946;
_gid=GA1.2.1396295264.1552431132; _gcl_au=1.1.404074092.1552323525;
_fbp=fb.1.1552323526191.52071667;CustomCookie=WebInspect141622ZXE000CE7833EE4CBCB1B0690CD295CDC0YC8A5
```

Attack Response:

```
HTTP/1.1 200 OK
Date: Wed, 13 Mar 2019 00:23:29 GMT
X-Frame-Options: SAMEORIGIN
Content-Type: text/html; charset=utf-8
Content-Length: 16129
ETag: W/"3f01-Sn+DneAOjpxnqwVNVujOl+91Y3U"
Set-Cookie: connect.sid=s%3A2elaWPMp1jpy7vDuK3ggeUpv3kIzZWuL.lbXc8mr31%2FQJ987wrTAX8m2K%
2FKYWnisjECietMsNrjw; Path=/; HttpOnly; Secure
Set-Cookie: ADRUM_BT=R:0|g:070481de-7715-4e9f-bd7f-29b2acf368e95648|s:f|n:PIT_948e56b2-cdee-4f42-bf8d-
46318aebf03f; Path=/; Expires=Wed, 13 Mar 2019 00:23:59 GMT; Secure
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Set-Cookie: BIGipServer~UNIX_Systems~PIT_DDINS-SSL=2711618826.64288.0000; path=/; Httponly; Secure

<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <meta http-equiv="X-UA-Compatible" content="IE=edge" />
    <title>Get A Quote</title>

    <!-- Page-hiding snippet (recommended)  -->
    <style>.async-hide { opacity: 0 !important} </style>
    <script>(function(a,s,y,n,c,h,i,d,e){s.className+=' '+y;h.start=1*new Date;
        h.end=i=function(){s.className=s.className.replace(RegExp(' ?'+y),'')};
        (a[n]=a[n]||[]).hide=h;setTimeout(function(){i();h.end=null},c);h.timeout=c;
    })(window,document.documentElement,'async-hide','dataLayer',4000,
            {'GTM-NPRVDTC':true});</script>
    <!-- Modified Analytics tracking code with Optimize plugin -->
    <script type="text/javascript">
        (function(i, s, o, g, r, a, m) {
            i['GoogleAnalyticsObject'] = r;
            i[r] = i[r] || function() {
                        (i[r].q = i[r].q || []).push(arguments)
                    }, i[r].l = 1 * new Date();
            a = s.createElement(o), m = s.getElementsByTagName(o)[0];
            a.async = 1;
            a.src = g;
            m.parentNode.insertBefore(a, m)
        })(window, document, 'script', '//www.google-analytics.com/analytics.js', 'ga');
        ga('create', 'UA-9398012-1', 'auto');
        ga('require', 'GTM-NPRVDTC', 'auto');
        var dnt= navigator.doNotTrack || window.doNotTrack || window.msDoNotTrack;
        ga('set', 'dimension9', dnt);
        ga('send', 'pageview');
    </script>

        <script type="text/javascript" src="https://maps.googleapis.com/maps/api/js?client=gme-
deltadentalofcalifornia&libraries=places"></script>
        <script type="text/javascript" src="/shopping/js/jquery-8101d596b2.js"></script>

    <script>window['adrum-start-time'] = new Date().getTime();</script>
    <script type="text/javascript" src="/shopping/js/html5shiv-40bd440d29.min.js" async></script>


        <link rel="stylesheet" type="text/css" href="/shopping/styles/style-67c2fc579a.css">
```

```
  <link rel="stylesheet" type="text/css" href="//cloud.typography.com/6549574/670548/css/fonts.css" />
</head>
<body>
<!-- MAIN CONTENT -->
        <header class="shopping-header-title">

                                <a class="back-arrow-link" id="shoppingBack"
href="https://pit.deltadentalins.com/"><i class="icon  icon-back-arrow-shopping" aria-label="shopping back arrow icon"
><span class="visually-hidden">back to previous page</span></i>
<span class="visually-hidden">back to previous page</span></a>

                        <div class="main-content">
                                <h1 class="shopping-header-content">
                                        Get a Quote
                                </h1>
                        </div>
                        </header>


<main role="main" class="main-content container page-control get-a-quote">
 <div class="main-container-inner">
  <div class="top-heading-section">
    <div class="error-container global-margin">
    </div>
   <div class="summary grey-text">
    We need a little more information to give you a quote.
   </div>
  </div>
  <form id="get_a_quote" action="/shopping/delta/get-a-quote" method="post">
   <input type="hidden" id="jsEnabled" name="jsEnabled" value="false" />
     <label for="zip"   >What’s your ZIP code?</label>
     <input id="zip"  class="form-input quote_address_zip zip"  type="text" name="zip"  placeholder="ZIP code"      />

     <div class="inline-error-container"

...TRUNCATED...
```

File Names:

- https://pit.deltadentalins.com:443/shopping/delta/get-a-quote?issuerCode=DELTA

Medium **Insecure Deployment: OpenSSL**

Summary:

WebInspect has detected an SSL/TLS man-in-the-middle (MitM) vulnerability caused by a specially crafted SSL handshake message. Also known as OpenSSL ChangeCipherSpec (CCS) injection vulnerability, this bug is known to manifest in the OpenSSL implementation of the secure socket layer for versions earlier than 0.9.8za, 1.0.0 before 1.0.0m and 1.0.1 before 1.0.1h. A ChangeCipherSpec message signals peers to switch to a symmetric encryption during SSL handshake process after negotiating a master key to use for symmetric encryption. However, vulnerable versions of OpenSSL allow a CCS message before the master key is negotiated resulting in a zero length master key.

Execution:

To verify the vulnerability, determine the version of the OpenSSL library deployed on the application servers. The version information can be obtained by running the command openssl version. Note that the client needs to be directly connected to the server in order to test for the vulnerability. If a proxy server is present in the environment, it is recommended to test both the proxy and the application server for the vulnerability.

Implication:

Man-in-the-middle attackers may use this vulnerability to hijack and intercept secure SSL/TLS communication by issuing an early CCS message to client and server when both are using vulnerable instance of OpenSSL. This may allow the attacker to compromise the confidentiality of sensitive session data.

Fix:

Upgrade to latest OpenSSL version.

- OpenSSL 0.9.8 SSL/TLS users should upgrade to 0.9.8za or later.
- OpenSSL 1.0.0 SSL/TLS users should upgrade to 1.0.0m or later.
- OpenSSL 1.0.1 SSL/TLS users should upgrade to 1.0.1h or later.

Additionally, users should check for the possibility of an indirect dependency on the OpenSSL library via third party software. Upgrade any such instances according to vendor recommendations.

Reference:

- https://www.openssl.org/news/secadv_20140605.txt
- http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-0224

Attack Request:

```
GET /shopping/delta/plan-options/9801677?issuerCode=DELTA HTTP/1.1
Accept: */*
Referer: https://pit.deltadentalins.com/shopping/delta/plan-options?issuerCode=DELTA
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64; rv:30.0) Gecko/20100101 Firefox/30.0
Accept-Encoding: gzip, deflate
Host: pit.deltadentalins.com
Connection: Keep-Alive
Pragma: no-cache
Cookie: ADRUM_BT=R:74|g:070481de-7715-4e9f-bd7f-29b2acf368e95668|s:f|n:PIT_948e56b2-cdee-4f42-bf8d-
46318aebf03f; connect.sid=s%3A2elaWPMp1jpy7vDuK3ggeUpv3kIzZWuL.lbXc8mr31%2FQJ987wrTAX8m2K%
2FKYWnisjECietMsNrjw; BIGipServer~UNIX_Systems~PIT_DDINS-SSL=2711618826.64288.0000; QSI_HistorySession=https%
3A%2F%2Fpit.deltadentalins.com%2Fshopping%2Fdelta%2Fget-a-quote%3FissuerCode%3DDELTA~1552436615256%
7Chttps%3A%2F%2Fpit.deltadentalins.com%2Fshopping%2Fdelta%2Fplan-options%3FissuerCode%
3DDELTA~1552436637404; _ga=GA1.2.1222917316.1517435630; AMCV_E9D70FA75B3A18E80A495C49%
40AdobeOrg=1994364360%7CMCIDTS%7C17967%7CMCMID%7C22137510049759883710112622098244936722%
7CMCAAMLH-1552928317%7C9%7CMCAAMB-1552928317%
7CRKhpRz8krg2tLO6pguXWp5olkAcUniQYPHaMWWgdJ3xzPWQmdj0y%7CMCOPTOUT-1552330717s%7CNONE%7CvVersion%
7C3.4.0%7CMCAID%7CNONE%7CMCSYNCSOP%7C411-17946; _gid=GA1.2.1396295264.1552431132; _gat=1;
_gcl_au=1.1.404074092.1552323525; _fbp=fb.1.1552323526191.52071667; ADRUM=s=1552436639939&r=https%3A%2F%
2Fpit.deltadentalins.com%2Fshopping%2Fdelta%2Fplan-options%3F-
1555445888;CustomCookie=WebInspect141622ZXE000CE7833EE4CBCB1B0690CD295CDC0YC8A5
```

Attack Response:

```
HTTP/1.1 200 OK
Date: Wed, 13 Mar 2019 00:24:00 GMT
X-Frame-Options: SAMEORIGIN
Content-Type: text/html; charset=utf-8
Content-Length: 15373
ETag: W/"3c0d-aIVxyEGRzU8Gxs1nvXTKWgGV438"
Set-Cookie: ADRUM_BT=R:75|g:070481de-7715-4e9f-bd7f-29b2acf368e95669|s:f|n:PIT_948e56b2-cdee-4f42-bf8d-
46318aebf03f; Path=/; Expires=Wed, 13 Mar 2019 00:24:30 GMT; Secure
Keep-Alive: timeout=5, max=98
Connection: Keep-Alive

<!DOCTYPE html>
<html lang="en">
<head>
  <meta charset="UTF-8">
  <meta name="viewport" content="width=device-width, initial-scale=1.0">
  <meta http-equiv="X-UA-Compatible" content="IE=edge" />
  <title>Plan Details</title>

  <!-- Page-hiding snippet (recommended)  -->
  <style>.async-hide { opacity: 0 !important} </style>
  <script>(function(a,s,y,n,c,h,i,d,e){s.className+=' '+y;h.start=1*new Date;
    h.end=i=function(){s.className=s.className.replace(RegExp(' ?'+y),'')};
    (a[n]=a[n]||[]).hide=h;setTimeout(function(){i();h.end=null},c);h.timeout=c;
  })(window,document.documentElement,'async-hide','dataLayer',4000,
      {'GTM-NPRVDTC':true});</script>
  <!-- Modified Analytics tracking code with Optimize plugin -->
  <script type="text/javascript">
    (function(i, s, o, g, r, a, m) {
      i['GoogleAnalyticsObject'] = r;
      i[r] = i[r] || function() {
            (i[r].q = i[r].q || []).push(arguments)
          }, i[r].l = 1 * new Date();
      a = s.createElement(o), m = s.getElementsByTagName(o)[0];
      a.async = 1;
      a.src = g;
      m.parentNode.insertBefore(a, m)
    })(window, document, 'script', '//www.google-analytics.com/analytics.js', 'ga');
    ga('create', 'UA-9398012-1', 'auto');
    ga('require', 'GTM-NPRVDTC', 'auto');
    var dnt= navigator.doNotTrack || window.doNotTrack || window.msDoNotTrack;
    ga('set', 'dimension9', dnt);
    ga('send', 'pageview');
  </script>
```

```
        <script type="text/javascript" src="https://maps.googleapis.com/maps/api/js?client=gme-
deltadentalofcalifornia&libraries=places"></script>
        <script type="text/javascript" src="/shopping/js/jquery-8101d596b2.js"></script>

    <script>window['adrum-start-time'] = new Date().getTime();</script>
    <script type="text/javascript" src="/shopping/js/html5shiv-40bd440d29.min.js" async></script>


        <link rel="stylesheet" type="text/css" href="/shopping/styles/style-67c2fc579a.css">


    <link rel="stylesheet" type="text/css" href="//cloud.typography.com/6549574/670548/css/fonts.css" />
</head>
<body>
<!-- MAIN CONTENT -->
              <header class="shopping-header-title">

                                            <a class="back-arrow-link" id="shoppingBack" href="/shopping/delta/plan-options?
issuerCode=DELTA"><i class="icon  icon-back-arrow-shopping" aria-label="shopping back arrow icon" ><span
class="visually-hidden">back to previous page</span></i>
<span class="visually-hidden">back to previous page</span></a>

                              <div class="main-content">
                                            <h1 class="shopping-header-content">
                                                          Plan Details
                                            </h1>
                              </div>
                              </header>


<main role="main" class="main-content container page-control plan-details">
   <div class="error-container global-margin">
</div>

  <form id="buyPlan" action="/enroll/delta/personal-info" onSubmit="planDetails.buildGATrackerObj()" method="POST">

       <section class="shopping-details-hero">
    <div class="shopping-details-hero__inner">
          <div class="shopping-details-hero__details">
            <h1>Delta Dental PPO Individual - Basic Plan</h1>
            <h3>
              <span aria-hidden="true">
                $33
                <sup>91</sup>
              </span>
              <span class="visually-hidden">33 dollars and 91 cents</span>
              <p class="per_month">per month</p>
              <p class="enroll_fee">$10 Enrollment Fee</p>

            </h3>
          </div>
        <div class="shopping-details-hero__cta">
              <input type="hidden" id="planType" name="planType" value="PPO" />


...TRUNCATED...
```

File Names:
- https://pit.deltadentalins.com:443/shopping/delta/plan-options/9801677?issuerCode=DELTA

Medium	**Insecure Transport: Weak SSL Protocol**

Summary:

Fortify WebInspect has detected support for Transport Layer Security Protocol (TLS) 1.1 protocol on the target server. NIST publication 800-52 revision 1 recommends all web applications to prefer Transport Layer Security Protocol version 1.2 (TLS 1.2) and mandates government agencies to develop a migration plan for TLS1.2 by January 2015. TLS1.1 mandates a combination of MD5 and SHA1 for the hash function, which leads to conclusion that strength of TLS1.1 depends largely on the strength of SHA1. MD5 is generally known to be weak. SHA1 use is being phased out. NIST Special Publication 800-131A deprecated the use of SHA-1 in digital signature starting January 2014.

Execution:

The list of supported SSL/TLS protocols can be obtained by running the server analyzer tool from Fortify Security Toolkit supplied with Fortify WebInspect against the target server.

Implication:

Weak TLS/SSL protocols may exhibit any or all of the following properties:

- No protection against man-in-the-middle (MitM) attacks
- Same key used for authentication and encryption
- Weak message authentication control
- No protection against TCP connection closing

These properties can allow an attacker to intercept, modify and tamper with sensitive data.

Fix:

Have a migration plan in place for all sites to exclusively use TLS1.2 and above. Disable support for the TLS 1.1 protocol on the server. Instead, TLSv1.2 and above should be used.

- For Apache, modify the following lines in the server configuration
- SSL Protocol ALL –SSLv2 -SSLv3 -TLSv1 –TLSv1.1

- For Nginx, modify the following lines in server configuration:

- SSL_Protocols TLSv1.2

- For IIS, please refer to Microsoft Knowledge Base Articles:

- https://technet.microsoft.com/library/security/3009008

For other servers, please refer to vendor specific documentation.

Reference:

NIST Special Publication 800-131A
NIST Special Publication 800-52r1

Attack Request:

```
GET /shopping/delta/get-a-quote?issuerCode=DELTA HTTP/1.1
Accept: */*
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64; rv:30.0) Gecko/20100101 Firefox/30.0
Accept-Encoding: gzip, deflate
Host: pit.deltadentalins.com
Connection: Keep-Alive
Pragma: no-cache
Cookie: _ga=GA1.2.1222917316.1517435630; AMCV_E9D70FA75B3A18E80A495C49%40AdobeOrg=1994364360%
7CMCIDTS%7C17967%7CMCMID%7C22137510049759883710112622098244936722%7CMCAAMLH-1552928317%7C9%
7CMCAAMB-1552928317%7CRKhpRz8krg2tLO6pguXWp5olkAcUniQYPHaMWWgdJ3xzPWQmdj0y%7CMCOPTOUT-
1552330717s%7CNONE%7CvVersion%7C3.4.0%7CMCAID%7CNONE%7CMCSYNCSOP%7C411-17946;
_gid=GA1.2.1396295264.1552431132; _gcl_au=1.1.404074092.1552323525;
_fbp=fb.1.1552323526191.52071667;CustomCookie=WebInspect141622ZXE000CE7833EE4CBCB1B0690CD295CDC0YC8A5
```

Attack Response:

```
HTTP/1.1 200 OK
Date: Wed, 13 Mar 2019 00:23:29 GMT
X-Frame-Options: SAMEORIGIN
Content-Type: text/html; charset=utf-8
Content-Length: 16129
ETag: W/"3f01-Sn+DneAOjpxnqwVNVujOl+91Y3U"
Set-Cookie: connect.sid=s%3A2elaWPMp1jpy7vDuK3ggeUpv3kIzZWuL.lbXc8mr31%2FQJ987wrTAX8m2K%
2FKYWnisjECietMsNrjw; Path=/; HttpOnly; Secure
```

```
Set-Cookie: ADRUM_BT=R:0|g:070481de-7715-4e9f-bd7f-29b2acf368e95648|s:f|n:PIT_948e56b2-cdee-4f42-bf8d-
46318aebf03f; Path=/; Expires=Wed, 13 Mar 2019 00:23:59 GMT; Secure
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Set-Cookie: BIGipServer~UNIX_Systems~PIT_DDINS-SSL=2711618826.64288.0000; path=/; Httponly; Secure

<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <meta http-equiv="X-UA-Compatible" content="IE=edge" />
    <title>Get A Quote</title>

    <!-- Page-hiding snippet (recommended)  -->
    <style>.async-hide { opacity: 0 !important} </style>
    <script>(function(a,s,y,n,c,h,i,d,e){s.className+=' '+y;h.start=1*new Date;
        h.end=i=function(){s.className=s.className.replace(RegExp(' ?'+y),'')};
        (a[n]=a[n]||[]).hide=h;setTimeout(function(){i();h.end=null},c);h.timeout=c;
    })(window,document.documentElement,'async-hide','dataLayer',4000,
            {'GTM-NPRVDTC':true});</script>
    <!-- Modified Analytics tracking code with Optimize plugin -->
    <script type="text/javascript">
        (function(i, s, o, g, r, a, m) {
            i['GoogleAnalyticsObject'] = r;
            i[r] = i[r] || function() {
                        (i[r].q = i[r].q || []).push(arguments)
                    }, i[r].l = 1 * new Date();
            a = s.createElement(o), m = s.getElementsByTagName(o)[0];
            a.async = 1;
            a.src = g;
            m.parentNode.insertBefore(a, m)
        })(window, document, 'script', '//www.google-analytics.com/analytics.js', 'ga');
        ga('create', 'UA-9398012-1', 'auto');
        ga('require', 'GTM-NPRVDTC', 'auto');
        var dnt= navigator.doNotTrack || window.doNotTrack || window.msDoNotTrack;
        ga('set', 'dimension9', dnt);
        ga('send', 'pageview');
    </script>

        <script type="text/javascript" src="https://maps.googleapis.com/maps/api/js?client=gme-
deltadentalofcalifornia&libraries=places"></script>
        <script type="text/javascript" src="/shopping/js/jquery-8101d596b2.js"></script>

    <script>window['adrum-start-time'] = new Date().getTime();</script>
    <script type="text/javascript" src="/shopping/js/html5shiv-40bd440d29.min.js" async></script>


        <link rel="stylesheet" type="text/css" href="/shopping/styles/style-67c2fc579a.css">


    <link rel="stylesheet" type="text/css" href="//cloud.typography.com/6549574/670548/css/fonts.css" />
</head>
<body>
<!-- MAIN CONTENT -->
               <header class="shopping-header-title">

                                                            <a class="back-arrow-link" id="shoppingBack"
href="https://pit.deltadentalins.com/"><i class="icon  icon-back-arrow-shopping" aria-label="shopping back arrow icon"
><span class="visually-hidden">back to previous page</span></i>
<span class="visually-hidden">back to previous page</span></a>

                                            <div class="main-content">
                                                            <h1 class="shopping-header-content">
                                                                            Get a Quote
                                                            </h1>
                                            </div>
                                            </header>


<main role="main" class="main-content container page-control get-a-quote">
  <div class="main-container-inner">
    <div class="top-heading-section">
        <div class="error-container global-margin">
        </div>
      <div class="summary grey-text">
        We need a little more information to give you a quote.
      </div>
    </div>
    <form id="get_a_quote" action="/shopping/delta/get-a-quote" method="post">
      <input type="hidden" id="jsEnabled" name="jsEnabled" value="false" />
          <label for="zip"   >What’s your ZIP code?</label>
          <input id="zip"  class="form-input quote_address_zip zip"  type="text" name="zip"  placeholder="ZIP code"      />

          <div class="inline-error-container"

...TRUNCATED...
```

File Names:

- https://pit.deltadentalins.com:443/shopping/delta/get-a-quote?issuerCode=DELTA

Low

Cookie Security: HTTPOnly not Set

Summary:

The web application does not utilize HTTP only cookies. This is a new security feature introduced by Microsoft in IE 6 SP1 to mitigate the possibility of a successful Cross-Site scripting attack by not allowing cookies with the HTTP only attribute to be accessed via client-side scripts. Recommendations include adopting a development policy that includes the utilization of HTTP only cookies, and performing other actions such as ensuring proper filtration of user-supplied data, utilizing client-side validation of user supplied data, and encoding all user supplied data to prevent inserted scripts being sent to end users in a format that can be executed.

Reference:

References:
https://social.msdn.microsoft.com/Search/en-US?query=HTTPOnly%20Cookie&emptyWatermark=true&ac=5

Attack Request:

```
GET /enroll/delta/payment HTTP/1.1
Accept: */*
Referer: https://pit.deltadentalins.com/enroll/delta/dependents
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64; rv:30.0) Gecko/20100101 Firefox/30.0
Accept-Encoding: gzip, deflate
Host: pit.deltadentalins.com
Connection: Keep-Alive
Cache-Control: no-cache
Pragma: no-cache
Cookie: ADRUM_BT=R:54|g:6111d309-18ad-4445-b1c0-0480d34b88ae5686|n:PIT_948e56b2-cdee-4f42-bf8d-46318aebf03f;
connect.sid=s%3A2elaWPMp1jpy7vDuK3ggeUpv3kIzZWuL.lbXc8mr31%2FQJ987wrTAX8m2K%2FKYWnisjECietMsNrjw;
BIGipServer~UNIX_Systems~PIT_DDINS-SSL=2711618826.64288.0000; QSI_HistorySession=https%3A%2F%
2Fpit.deltadentalins.com%2Fshopping%2Fdelta%2Fget-a-quote%3FissuerCode%3DDELTA~1552436615256%7Chttps%3A%
2F%2Fpit.deltadentalins.com%2Fshopping%2Fdelta%2Fplan-options%3FissuerCode%3DDELTA~1552436637404%7Chttps%
3A%2F%2Fpit.deltadentalins.com%2Fshopping%2Fdelta%2Fplan-options%2F9801677%3FissuerCode%
3DDELTA~1552436642618%7Chttps%3A%2F%2Fpit.deltadentalins.com%2Fenroll%2Fdelta%2Fpersonal-
info~1552436651514; _ga=GA1.2.1222917316.1517435630; AMCV_E9D70FA75B3A18E80A495C49%
40AdobeOrg=1994364360%7CMCIDTS%7C17967%7CMCMID%7C22137510049759883710112622098244936722%
7CMCAAMLH-1552928317%7C9%7CMCAAMB-1552928317%
7CRKhpRz8krg2tLO6pguXWp5olkAcUniQYPHaMWWgdJ3xzPWQmdj0y%7CMCOPTOUT-1552330717s%7CNONE%7CvVersion%
7C3.4.0%7CMCAID%7CNONE%7CMCSYNCSOP%7C411-17946; _gid=GA1.2.1396295264.1552431132; _gat=1;
_gcl_au=1.1.404074092.1552323525; _fbp=fb.1.1552323526191.52071667; ADRUM=s=1552436717420&r=https%3A%2F%
2Fpit.deltadentalins.com%2Fenroll%2Fdelta%2Fdependents%
3F0;CustomCookie=WebInspect141622ZXE000CE7833EE4CBCB1B0690CD295CDC0YC8A5
```

Attack Response:

```
HTTP/1.1 200 OK
Date: Wed, 13 Mar 2019 00:25:18 GMT
```

```
X-Frame-Options: SAMEORIGIN
Cache-Control: no-cache
Cache-Control: no-store
Content-Type: text/html; charset=utf-8
Content-Length: 32617
ETag: W/"7f69-5pNOkhY1XdEv5GluqGw66MhNTSs"
Set-Cookie:
ADRUM_BT=R:54|g:6111d309-18ad-4445-b1c0-0480d34b88ae5687|n:PIT_948e56b2-cdee-4f42-bf8d-46318aebf03f; Path=/;
Expires=Wed, 13 Mar 2019 00:25:48 GMT; Secure
Keep-Alive: timeout=5, max=95
Connection: Keep-...TRUNCATED...
```

File Names:

- https://pit.deltadentalins.com:443/enroll/delta/payment
- https://pit.deltadentalins.com:443/enroll/delta/review
- https://pit.deltadentalins.com:443/enroll/api/v1/cx/enrollment/addressCleanse
- https://pit.deltadentalins.com:443/shopping/delta/get-a-quote?issuerCode=DELTA
- https://pit.deltadentalins.com:443/enroll/delta/personal-info
- https://pit.deltadentalins.com:443/shopping/delta/plan-options/9801677?issuerCode=DELTA
- https://pit.deltadentalins.com:443/enroll/delta/dependents
- https://pit.deltadentalins.com:443/shopping/delta/plan-options?issuerCode=DELTA
- https://pit.deltadentalins.com:443/enroll/delta/receipt

Low

Web Server Misconfiguration: Server Error Message

Summary:

A server error response was detected. The server could be experiencing errors due to a misbehaving application, a misconfiguration, or a malicious value sent during the auditing process. While error responses in and of themselves are not dangerous, per se, the error responses give attackers insight into how the application handles error conditions. Errors that can be remotely triggered by an attacker can also potentially lead to a denial of service attack or other more severe vulnerability. Recommendations include designing and adding consistent error handling mechanisms which are capable of handling any user input to your web application, providing meaningful detail to end-users, and preventing error messages that might provide information useful to an attacker from being displayed.

Implication:

The server has issued a 500 error response. While the body content of the error page may not expose any information about the technical error, the fact that an error occurred is confirmed by the 500 status code. Knowing whether certain inputs trigger a server error can aid or inform an attacker of potential vulnerabilities.

Fix:

For Security Operations:

Server error messages, such as "File Protected Against Access", often reveal more information than intended. For instance, an attacker who receives this message can be relatively certain that file exists, which might give him the information he needs to pursue other leads, or to perform an actual exploit. The following recommendations will help to ensure that a potential attacker is not deriving valuable information from any server error message that is presented.

- Uniform Error Codes: Ensure that you are not inadvertently supplying information to an attacker via the use of inconsistent or "conflicting" error messages. For instance, don't reveal unintended information by utilizing error messages such as Access Denied, which will also let an attacker know that the file he seeks actually exists. Have consistent terminology for files and folders that do exist, do not exist, and which have read access denied.
- Informational Error Messages: Ensure that error messages do not reveal too much information. Complete or partial paths, variable and file names, row and column names in tables, and specific database errors should never be revealed to the end user. Remember, an attacker will gather as much information as possible, and then add pieces of seemingly innocuous information together to craft a method of attack.
- Proper Error Handling: Utilize generic error pages and error handling logic to inform end users of potential problems. Do not provide system information or other data that could be utilized by an attacker when orchestrating an attack.

Removing Detailed Error Messages

Find instructions for turning off detailed error messaging in IIS at this link:

http://support.microsoft.com/kb/294807

For Development:

From a development perspective, the best method of preventing problems from arising from server error messages is to adopt secure programming techniques that prevent problems that might arise from an attacker discovering too much information about the architecture and design of your web application. The following recommendations can be used as a basis for that.

- Stringently define the data type (for instance, a string, an alphanumeric character, etc) that the application will accept.
- Use what is good instead of what is bad. Validate input for improper characters.
- Do not display error messages to the end user that provide information (such as table names) that could be utilized in orchestrating an attack.
- Define the allowed set of characters. For instance, if a field is to receive a number, only let that field accept numbers.
- Define the maximum and minimum data lengths for what the application will accept.
- Specify acceptable numeric ranges for input.

For QA:

The best course of action for QA associates to take is to ensure that the error handling scheme is consistent. Do you receive a different type of error for a file that does not exist as opposed to a file that does? Are phrases like "Permission Denied" utilized which could reveal the existence of a file to an attacker? Inconsistent methods of dealing with errors gives an attacker a very powerful way of gathering information about your web application.

Reference:

Apache:
Security Tips for Server Configuration
Protecting Confidential Documents at Your Site
Securing Apache - Access Control

Microsoft:
How to set required NTFS permissions and user rights for an IIS 5.0 Web server
Default permissions and user rights for IIS 6.0
Description of Microsoft Internet Information Services (IIS) 5.0 and 6.0 status codes

Attack Request:

```
GET /shopping/delta/PRcx^bx^bxdfdfcaaccRP/WINDOWS/win.ini?issuerCode=DELTA HTTP/1.1
Accept: */*
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64; rv:30.0) Gecko/20100101 Firefox/30.0
Accept-Encoding: gzip, deflate
Host: pit.deltadentalins.com
Pragma: no-cache
Referer: https://pit.deltadentalins.com/shopping/delta/get-a-quote?issuerCode=DELTA
Connection: Keep-Alive
X-WIPP: AscVersion=18.20.178.0
X-Scan-Memo: Category="Audit.Attack"; SID="D29543D18C03447FD9AC4786A879D732";
PSID="07A4548C5A5C06E775F5ADBF385A45C5"; SessionType="AuditAttack"; CrawlType="None";
AttackType="QueryParamManipulation"; OriginatingEngineID="04922161-c0f3-47ba-8adf-397348373fed";
AttackSequence="1"; AttackParamDesc=""; AttackParamIndex="-1"; AttackParamSubIndex="0"; CheckId="11362";
Engine="Struts+Class+Loader+Manipulation"; SmartMode="NonServerSpecificOnly"; AttackString="";
AttackStringProps="Attack"; ThreadId="311"; ThreadType="AuditorStateRequestor";
X-RequestManager-Memo: RequestorThreadIndex="4"; sc="1"; ID="ed546dbe-cefe-416a-aad5-1d65aaa72477";
X-Request-Memo: ID="40d2796c-0b2f-46cf-9462-6c01922eb5f7"; sc="1"; ThreadId="311";
Cookie: _ga=GA1.2.1222917316.1517435630; AMCV_E9D70FA75B3A18E80A495C49%40AdobeOrg=1994364360%
7CMCIDTS%7C17967%7CMCMID%7C22137510049759883710112622098244936722%7CMCAAMLH-1552928317%7C9%
7CMCAAMB-1552928317%7CRKhpRz8krg2tLO6pguXWp5olkAcUniQYPHaMWWgdJ3xzPWQmdj0y%7CMCOPTOUT-
1552330717s%7CNONE%7CvVersion%7C3.4.0%7CMCAID%7CNONE%7CMCSYNCSOP%7C411-17946;
```

_gid=GA1.2.1396295264.1552431132; _gcl_au=1.1.404074092.1552323525;
_fbp=fb.1.1552323526191.52071667;CustomCookie=WebInspect141622ZXE000CE7833EE4CBCB1B0690CD295CDC0YC8A5

Attack Response:

HTTP/1.1 500 Internal Server Error
Date: Wed, 13 Mar 2019 00:...TRUNCATED...

File Names:

- https://pit.deltadentalins.com:443/shopping/delta/PRcx^bx^bxdfdfcaaccRP/WINDOWS/win.ini?issuerCode=D
- https://pit.deltadentalins.com:443/shopping/delta/get-a-quote
- https://pit.deltadentalins.com:443/shopping/delta/plan-options?issuerCode=DELTA
- https://pit.deltadentalins.com:443/shopping/delta/plan-options/
- https://pit.deltadentalins.com:443/enroll/api/v1/cx/enrollment/addressCleanse
- https://pit.deltadentalins.com:443/shopping/delta/plan-options/logs.htm
- https://pit.deltadentalins.com:443/enroll/delta/receipt
- https://pit.deltadentalins.com:443/enroll/delta/personal-info
- https://pit.deltadentalins.com:443/shopping/delta/plan-options/9801677?issuerCode=DELTA&class.classL
- https://pit.deltadentalins.com:443/shopping/delta/plan-options/logs.asp
- https://pit.deltadentalins.com:443/enroll/delta/payment
- https://pit.deltadentalins.com:443/shopping/delta/PRcx^bx^bxdfdfcaaccRP/etc/passwd?issuerCode=DELTA
- https://pit.deltadentalins.com:443/enroll/delta/review
- https://pit.deltadentalins.com:443/enroll/delta/dependents

Low

Cache Management: Insecure Policy

Summary:

WebInspect has detected a potentially unsafe cache control policy for secure content. While content transmitted over an SSL/TLS channel is expected to guarantee confidentiality, administrators must nonetheless ensure that caching of sensitive content is disabled unless absolutely needed. The misconception that secure content caching is disabled by default by user-agents could cause the application to fail the organization’s cache policy by leaving the secure content cacheable by browsers. Unsafe specification such as Cache-Control: public would instruct the browser to persistently cache the content on the hard drive. Caching can be prevented by specifying one of the following three directives in the response headers

- Cache-control: private
- Cache-Control: no-cache
- Cache-Control: no-store

Execution:

Send a request to https://pit.deltadentalins.com:443/enroll/js/jquery-24ae1ca673.validate.min.js and inspect the Cache-Control header value.

Implication:

Insecure caching policies could lead to content spoofing or information theft.

SSL provides secure encrypted channel to transfer information from source to user. The information server over SSL is considered sensitive and trusted to be only available to requestor. However, caching these content on disk in temporary internet files or in intermediate proxy server can compromise that trust by exposing it to everyone who has access to these temporary storage or proxy cache. Content served over SSL should have cache disabled.

Fix:

Set Cache-Control directive to private, no-cache and/or no-store.

private
This directive allows the server to prevent a shared cache from caching responses that are intended for a single user. The mechanism can be used to ensure that privileged information is not accidentally leaked to unauthorized users. The directive may still allow caching of responses by non-shared caches.

no-cache
For sensitive resources requiring user authentication, servers can send the no-cache directive to prevent caches from serving a cached response without first requiring the user agent to validate the user identity. This directive can be specified with or

without field names. When no field names are included, this directive applies to the entire request or response.
When one or more field names are specified in the no-cache directive, the response is can be cached but the specified field(s) must be excluded. If the response must include the specified field, then the cache must ensure that the request triggers a revalidation with the origin server.
Example: Cache-Control: no-cache="Set-Cookie"
This directive can be used to ensure sensitive information leakage by requiring the server to confirm the user identity before serving the protected information.

no-store
To completely disable caching of requests or responses, the server must specify the no-store directive in the Cache-Control header. This directive applies to the entire request and response regardless of whether the directive is sent in the request or the response.

Reference:

Server Configuration:
IIS
Apache

HTTP 1.1 Specification:
HTTP Header Field Definitions

OWASP:
Browser Cache FAQ

HTTP Caching:
Tutorial

Attack Request:

```
GET /enroll/js/jquery-24ae1ca673.validate.min.js HTTP/1...TRUNCATED...
```

Attack Response:

```
HTTP/1.1 200 OK
Date: Wed, 13 Mar 2019 00:24:05 GMT
S...TRUNCATED...
```

File Names:

- https://pit.deltadentalins.com:443/enroll/js/jquery-24ae1ca673.validate.min.js
- https://pit.deltadentalins.com:443/enroll/js/receipt-a33e12cc02.js
- https://pit.deltadentalins.com:443/enroll/js/zippopupsingle-6124fbf8cb.js
- https://pit.deltadentalins.com:443/enroll/js/additional-methods-d95f4f840a.min.js
- https://pit.deltadentalins.com:443/shopping/delta/get-a-quote?issuerCode=DELTA
- https://pit.deltadentalins.com:443/enroll/delta/payment
- https://pit.deltadentalins.com:443/enroll/js/pit-adrum-3725132db5.js
- https://pit.deltadentalins.com:443/enroll/api/v1/cx/enrollment/addressCleanse
- https://pit.deltadentalins.com:443/enroll/js/html5shiv-40bd440d29.min.js
- https://pit.deltadentalins.com:443/enroll/js/es5-shim-136920ce3d.min.js
- https://pit.deltadentalins.com:443/enroll/js/review-1a1c100d01.js
- https://pit.deltadentalins.com:443/shopping/js/planDetails-ca524498cf.js
- https://pit.deltadentalins.com:443/enroll/js/jquery-ab3696dee1.payment.js
- https://pit.deltadentalins.com:443/enroll/js/feedback-763706aa40.js
- https://pit.deltadentalins.com:443/enroll/js/jquery-3b5470c70d.mask.min.js
- https://pit.deltadentalins.com:443/shopping/delta/plan-options/9801677?issuerCode=DELTA
- https://pit.deltadentalins.com:443/enroll/js/common-c257863844.js
- https://pit.deltadentalins.com:443/enroll/delta/review
- https://pit.deltadentalins.com:443/enroll/js/payment-732a6decc4.js
- https://pit.deltadentalins.com:443/enroll/delta/dependents
- https://pit.deltadentalins.com:443/enroll/js/personal-info-300c5872da.js
- https://pit.deltadentalins.com:443/shopping/js/planOptions-615ccf3ae8.js
- https://pit.deltadentalins.com:443/enroll/js/jquery-8101d596b2.js

- https://pit.deltadentalins.com:443/enroll/js/dependents-93567b86ba.js
- https://pit.deltadentalins.com:443/enroll/js/validation-3a3a507f31.js
- https://pit.deltadentalins.com:443/shopping/delta/plan-options?issuerCode=DELTA
- https://pit.deltadentalins.com:443/enroll/locale-based/en/US/client-data.json
- https://pit.deltadentalins.com:443/enroll/delta/personal-info

Low

Insecure Transport: HSTS not Set

Summary:

Http Strict Transport Security (HSTS) policy enables web applications to enforce web browsers to restrict communication with the server over an encrypted SSL/TLS connection for a set period. Policy is declared via special Strict Transport Security response header. Encrypted connection protects sensitive user and session data from attackers eavesdropping on network connection.
Consider following attack scenarios:

- Users often omit the URI scheme i.e. https:// when typing a URL in location bar to access a website. Also third party websites can link to the site using the “http” scheme instead of "”https”. This could result in an initial connection to a HTTPS-enabled site over an unencrypted channel. An eavesdropping attacker can hijack this unencrypted connection and replace the intended use of HTTPS protocol with HTTP in an attack known as SSLStrip, granting unauthorized access to all subsequent traffic.
- Websites often transfer non-sensitive resources such as help documents over an unencrypted HTTP connection. Any cookies without a secure flag are sent along with such requests potentially disclosing sensitive user and session data to eavesdropper.
- Man-in-the-Middle attacks that exploit user tendencies to override invalid certification warnings, e.g. SSLSniff.

For web sites configured with an accurate HSTS policy, browsers automatically upgrade any HTTP connections to HTTPS. Furthermore, browsers prevent users from overriding any host certificate warnings. HSTS offers an effective defense against above attack scenarios.

Execution:

Access location https://pit.deltadentalins.com:443/shopping/js/planOptions-615ccf3ae8.js and notice the absence of the Strict Transport Security header in the HTTP response.

Implication:

A successful MiTM attack such as SSLStrip or SSLsniff can lead to the compromise of sensitive user data such as financial information, Social Security Number, personal information etc. as well as grant unauthorized access to user accounts enabling attackers to perform privileged actions on client’s behalf.

Fix:

Configure the web application under test to include Strict Transport Security header in every response generated by an HTTPS-enabled site. Any HTTP version of site on the same domain should permanently redirect to the secure encrypted site. Header should not be added to HTTP response as browsers will ignore it.

It is important to note that this header does not prevent from above mentioned attack scenarios during the very first connection to the site or any connections established after the set period has expired. To prevent such a scenario, the site must be added to the pre-loaded HSTS hosts list embedded in both Google Chrome and Mozilla Firefox browsers.

Reference:

http://tools.ietf.org/html/rfc6797

Attack Request:

```
GET /shopping/js/planOptions-615ccf3ae8.js HTTP/1.1
Accept: */*
Referer: https://pit.deltadentalins.com/shopping/delta/plan-options?issuerCode=DELTA
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64; rv:30.0) Gecko/20100101 Firefox/30.0
Accept-Encoding: gzip, deflate
Host: pit.deltadentalins.com
Connection: Keep-Alive
Pragma: no-cache
Cookie: ADRUM_BT=R:74|g:070481de-7715-4e9f-bd7f-29b2acf368e95668|s:f|n:PIT_948e56b2-cdee-4f42-bf8d-
46318aebf03f; connect.sid=s%3A2elaWPMp1jpy7vDuK3ggeUpv3kIzZWuL.lbXc8mr31%2FQJ987wrTAX8m2K%
2FKYWnisjECietMsNrjw; BIGipServer~UNIX_Systems~PIT_DDINS-SSL=2711618826.64288.0000; QSI_HistorySession=https%
3A%2F%2Fpit.deltadentalins.com%2Fshopping%2Fdelta%2Fget-a-quote%3FissuerCode%3DDELTA~1552436615256;
_ga=GA1.2.1222917316.1517435630; AMCV_E9D70FA75B3A18E80A495C49%40AdobeOrg=1994364360%7CMCIDTS%
7C17967%7CMCMID%7C22137510049759883710112622098244936722%7CMCAAMLH-1552928317%7C9%7CMCAAMB-
```

```
1552928317%7CRKhpRz8krg2tLO6pguXWp5olkAcUniQYPHaMWWgdJ3xzPWQmdj0y%7CMCOPTOUT-1552330717s%
7CNONE%7CvVersion%7C3.4.0%7CMCAID%7CNONE%7CMCSYNCSOP%7C411-17946;
_gid=GA1.2.1396295264.1552431132; _gat=1; _gcl_au=1.1.404074092.1552323525; _fbp=fb.1.1552323526191.52071667;
ADRUM=s=1552436632453&r=https%3A%2F%2Fpit.deltadentalins.com%2Fshopping%2Fdelta%2Fget-a-quote%3F-
1555445888;CustomCookie=WebInspect141622ZXE000CE7833EE4CBCB1B0690CD295CDC0YC8A5
```

Attack Response:

```
HTTP/1.1 200 OK
Date: Wed, 13 Mar 2019 00:23:55 GMT
Server: Apache
X-Frame-Options: SAMEORIGIN
Last-Modified: Thu, 07 Mar 2019 23:46:32 GMT
Accept-Ranges: bytes
Vary: Accept-Encoding
Content-Encoding: gzip
Cache-Control: max-age=86400, public
Content-Length: 1062
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: application/javascript

"use strict";var OPTIONS={rightPlans:$(".plan-options__right-side .plan-options-box").length,leftPlans:$(".plan-options__left-
side .plan-options-box").length,leftPlansHeight:$(".plan-options__left-side .plan-options-box").height
(),rightPlansHeight:$(".plan-options__right-side .plan-options-box").height(),init:function(){OPTIONS.moreThanOneColumn
(),OPTIONS.equalizeColumns()},moreThanOneColumn:function(){0===OPTIONS.rightPlans?($(".plan-options__right-
side").remove(),$(".plan-options__left-side").addClass("plan-options__single-col")):!
OPTIONS.rightPlans&&OPTIONS.leftPlans<=2&&$(".plan-options__left-side").addClass("plan-options__two-
plan")},equalizeColumns:function(){940<$(window).width()?OPTIONS.rightPlansHeight>OPTIONS.leftPlansHeight?$(".plan-
options__left-side .plan-options-box").height
(OPTIONS.rightPlansHeight):OPTIONS.rightPlansHeight<OPTIONS.leftPlansHeight&&$(".plan-options__right-side .plan-options
-box").height(OPTIONS.leftPlansHeight):$(".plan-options-box").removeAttr("style")}};$(window).resize(function()
{OPTIONS.init()}),OPTIONS.init();
```

File Names:

- https://pit.deltadentalins.com:443/shopping/js/planOptions-615ccf3ae8.js

Informational

Cache Management: Headers

Summary:

The web server sent a Vary header, which indicates that server-driven negotiation was done to determine which content should be delivered. This may indicate that different content is available based on the headers in the HTTP request. Scan configuration recommendations include viewing the HTTP response to determine what criteria is used to negotiate content, and appending custom headers and values according to the negotiate criteria being used.

Fix:

For Development:
Verify your application does not display different content based on headers, and if necessary, re-scan with appropriate headers to ensure good coverage.

For Security Operations:
Evaluate if content negotiation is truly being used, and disable if it is unnecessary. Re-scan with appropriate headers to ensure good coverage.

For QA:
This requires a server or application configuration change. Contact Security Operations for assistance with the server.

Reference:

W3C RFC 2616 Header Field Definitions
http://www.w3.org/Protocols/rfc2616/rfc2616-sec14.html#sec14.44

Attack Request:

```
GET /enroll/js/validation-3a3a507f31.js HTTP/1.1
Accept: */*
Referer: https://pit.deltadentalins.com/enroll/delta/personal-info
Accept-Language: en-US
```

```
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64; rv:30.0) Gecko/20100101 Firefox/30.0
Accept-Encoding: gzip, deflate
Host: pit.deltadentalins.com
Connection: Keep-Alive
Pragma: no-cache
Cookie: ADRUM_BT=R:83|g:b653ad88-b9ca-41c5-a714-628552112b0d5682|n:PIT_948e56b2-cdee-4f42-bf8d-46318aebf03f;
connect.sid=s%3A2elaWPMp1jpy7vDuK3ggeUpv3kIzZWuL.lbXc8mr31%2FQJ987wrTAX8m2K%2FKYWnisjECietMsNrjw;
BIGipServer~UNIX_Systems~PIT_DDINS-SSL=2711618826.64288.0000; QSI_HistorySession=https%3A%2F%
2Fpit.deltadentalins.com%2Fshopping%2Fdelta%2Fget-a-quote%3FissuerCode%3DDELTA~1552436615256%7Chttps%3A%
2F%2Fpit.deltadentalins.com%2Fshopping%2Fdelta%2Fplan-options%3FissuerCode%3DDELTA~1552436637404%7Chttps%
3A%2F%2Fpit.deltadentalins.com%2Fshopping%2Fdelta%2Fplan-options%2F9801677%3FissuerCode%
3DDELTA~1552436642618; _ga=GA1.2.1222917316.1517435630; AMCV_E9D70FA75B3A18E80A495C49%
40AdobeOrg=1994364360%7CMCIDTS%7C17967%7CMCMID%7C22137510049759883710112622098244936722%
7CMCAAMLH-1552928317%7C9%7CMCAAMB-1552928317%
7CRKhpRz8krg2tLO6pguXWp5olkAcUniQYPHaMWWgdJ3xzPWQmdj0y%7CMCOPTOUT-1552330717s%7CNONE%7CvVersion%
7C3.4.0%7CMCAID%7CNONE%7CMCSYNCSOP%7C411-17946; _gid=GA1.2.1396295264.1552431132; _gat=1;
_gcl_au=1.1.404074092.1552323525; _fbp=fb.1.1552323526191.52071667; ADRUM=s=1552436644875&r=https%3A%2F%
2Fpit.deltadentalins.com%2Fshopping%2Fdelta%2Fplan-options%2F9801677%3F-
1555445888;CustomCookie=WebInspect141622ZXE000CE7833EE4CBCB1B0690CD295CDC0YC8A5
```

Attack Response:

```
HTTP/1.1 200 OK
Date: Wed, 13 Mar 2019 00:24:05 GMT
Server: Apache
X-Frame-Options: SAMEORIGIN
Last-Modified: Fri, 08 Mar 2019 22:53:59 GMT
Accept-Ranges: bytes
Vary: Accept-Encoding
Content-Encoding: gzip
Cache-Control: max-age=86400, public
Content-Length: 16658
Keep-Alive: timeout=5, max=99
Connection: Keep-Alive
Content-Type: application/javascript


$(document).ready(function(){$form.find("input").removeAttr("required"),$form.validate
(voptions),$("#zipCodeBias").length&&$("#zipCodeBias").validate(),$("input[type=text], input[type=email]").focusout
(function(){var e=$.trim($(this).val());$(this).val(e)})});var minAgePassed=!0,min_applicant_age_error_message="Applicant
must be over a certain age";function meetsMinAge(e){var a=$("#day").val(),r=$("#month").val(),t=$("#year").val
(),d=e,i=new Date;i.setFullYear(t,r-1,a-1);var n=new Date;return n.setFullYear(n.getFullYear()-d),minAgePassed=i<n}
function checkAge(e,a){var r=!1;if(thisForm=e.closest(".dep_form"),depIndex=e.attr("id").substring(e.attr("id").indexOf("_")
+1),handicapped=$(".dep_form:eq("+depIndex+")").find(".handicap"),year=thisForm.find(".year").val(),month=thisForm.find
(".month").val(),day=thisForm.find(".day").val(),relationship=thisForm.find(".relationship").val(),"Child"!
=relationship&&"Dependent Children"!=relationship||(r=!0),!year||year.length<4||!month||!day||!r)return!1;var t=new
Date;t.setFullYear(year,month-1,day);var d=new Date;if(d.setFullYear(d.getFullYear()-a),t<d){handicapped.removeClass
("hidden");var i="Age not correct";i="function"==typeof getHandicapErrorMsgOverride?getHandicapErrorMsgOverride
():client_data.errors.handiRequired_26,handicapped.find(".handicapped").is(":checked")?handicapped.find(".inline-error-
container").removeClass("error").html(""):handicapped.find(".inline-error-container").addClass("error").html(i)}else
handicapped.find(".handicapped").prop("checked",!1),handicapped.addClass("hidden"),handicapped.find(".inline-error-
container").removeClass("error").html("")}$.validator.methods.email=function(e,a){return this.optional(a)||/^(([^<>()\[\]
\\.,;:\s@"]+(\.[^<>()\[\]\\.,;:\s@"]+)*)|(".+"))@((\[[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}])|(([a-zA-Z\-0-9]+\.)+[a-
zA-Z]{2,}))$/.test(e)},$.validator.prototype.idOrName=function(e){return e.id},jQuery.validator.setDefaults
({errorElement:"a"}),$.validator.prototype.showLabel=function(e,a){var r,t,d,i,n=this.errorsFor(e),o=t
his.idOrName(e),s=$(e).attr("aria-describedby");n.length?(n.removeClass(this.settings.validClass).addClass
(this.settings.errorClass),n.html(a)):(r=n="a"===this.settings.errorElement?$("<"+this.settings.errorElement+">").attr
({id:o+"-error",href:"#"+o}).addClass(this.settings.errorClass).html(a||""):$("<"+this.settings.errorElement+">").attr
("id",o+"-error").addClass(this.settings.errorClass).html(a||""),this.settings.wrapper&&(r=n.hide().show().wrap
("<"+this.settings.wrapper+"/>").parent()),this.labelContainer.length?this.labelContainer.append
(r):this.settings.errorPlacement?this.settings.errorPlacement.call(this,r,$(e)):r.insertAfter(e),n.is("label")?n.attr
("for",o):0===n.parents("label[for='"+this.escapeCssMeta(o)+"']").length?(d=n.attr("id"),s?s.match(new RegExp
("\\b"+this.escapeCssMeta(d)+"\\b"))||(s+=" "+d):s=d,$(e).attr("aria-describedby",s),(t=this.groups[e.name])&&
(i=this,$.each(i.groups,function(e,a){a===t&&$("[name='"+i.escapeCssMeta(e)+"']",i.currentForm).attr("aria-
describedby",n.attr("id"))}))):n.is("label")&&n.attr("for",o)),!a&&this.settings.success&&(n.text(""),"string"==typeof
this.settings.success?n.addClass(this.settings.success):this.settings.success(n,e)),this.toShow=this.toShow.add(n)};var
client_data=$("#client_data_path").val();client_data&&$.getJSON(client_data,function(e){client_data=e,setValidations()});var
nameRegex=/^[a-zA-Z,'-]+$/,monthRegex=/[0-9]{1,2}/,monthCCRegex=/[0-9]{1,2}/,dayRegex=/[0-9]{1,2}/,yearRegex=/[0
-9]{4}/,yearCCRegex=/[0-9]{4}/,stateRegex=/[a-zA-Z]+(?:[\\s-][a-zA-Z]+)*/,zipRegex=/(\d{5}-\d{4})|(\d
{5})/,brokerRegex=/(\d+)/,creditName=/[a-zA-Z,' -]+/,creditRegex=/[\d-]{15,19}/,cvcRegex=/[\d]{3,4}/,pagename=

...TRUNCATED...
```

File Names:

- https://pit.deltadentalins.com:443/enroll/js/validation-3a3a507f31.js
- https://pit.deltadentalins.com:443/shopping/js/planOptions-615ccf3ae8.js
- https://pit.deltadentalins.com:443/enroll/delta/personal-info
- https://pit.deltadentalins.com:443/shopping/delta/get-a-quote
- https://pit.deltadentalins.com:443/enroll/locale-based/en/US/client-data.json?class['classLoader'].r

Informational **Insecure Deployment: Known Technology Fingerprint**

Summary:

WebInspect has determined that the target server supports the following TLS_RSA ciphers:

- **TLS_RSA_WITH_3DES_EDE_CBC_SHA (0xa)**
- **TLS_RSA_WITH_AES_256_CBC_SHA (0x35)**
- **TLS_RSA_WITH_AES_128_CBC_SHA (0x2f)**
- **TLS_RSA_WITH_CAMELLIA_128_CBC_SHA (0x41)**
- **TLS_RSA_WITH_CAMELLIA_256_CBC_SHA (0x84)**
- **TLS_RSA_WITH_AES_256_CBC_SHA256 (0x3d)**
- **TLS_RSA_WITH_AES_128_CBC_SHA256 (0x3c)**
- **TLS_RSA_WITH_AES_256_GCM_SHA384 (0x9d)**
- **TLS_RSA_WITH_AES_128_GCM_SHA256 (0x9c)**

While TLS_RSA itself is not vulnerable, several implementations of TLS_RSA cipher have been shown to be vulnerable to ROBOT Attack (Return Of Bleichenbacher's Oracle Threat). Bleichenbacher's is an adaptive chosen-ciphertext attack on the RSA PKCS#1v1.5 encryption standard. The vulnerability in the implementation of the RSA PKCS#1v1.5 algorithm allows an attacker to steal the private session key from a secure SSL/TLS session. The attacker can then use the key to compromise and decrypt recorded SSL/TLS sessions, leading to information disclosure and impersonation attacks.

Execution:

A list of ciphers supported by this server can be obtained by running ServerAnalyzer tool from the WebInspect toolkit. Note the presence of "TLS_RSA" ciphers in the list of supported ciphers.

Implication:

If a vulnerable version of the TLS_RSA exists on the server, the server may be vulnerable to ROBOT Attack which would allow an attacker to successfully decrypt a previously recorded SSL/TLS session, leading to information disclosure and impersonation attacks.

Fix:

Please refer to your vendor's documentation to check if the TLS_RSA version in use is vulnerable to ROBOT attack. If necessary please apply the required patch from the vendor to protect against this vulnerability.

Reference:

The ROBOT Attack
Return Of Bleichenbacher’s Oracle Threat

Attack Request:

```
GET /shopping/delta/get-a-quote?issuerCode=DELTA HTTP/1.1
Accept: */*
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64; rv:30.0) Gecko/20100101 Firefox/30.0
Accept-Encoding: gzip, deflate
Host: pit.deltadentalins.com
Connection: Keep-Alive
Pragma: no-cache
Cookie: _ga=GA1.2.1222917316.1517435630; AMCV_E9D70FA75B3A18E80A495C49%40AdobeOrg=1994364360%
7CMCIDTS%7C17967%7CMCMID%7C22137510049759883710112622098244936722%7CMCAAMLH-1552928317%7C9%
7CMCAAMB-1552928317%7CRKhpRz8krg2tLO6pguXWp5olkAcUniQYPHaMWWgdJ3xzPWQmdj0y%7CMCOPTOUT-
1552330717s%7CNONE%7CvVersion%7C3.4.0%7CMCAID%7CNONE%7CMCSYNCSOP%7C411-17946;
_gid=GA1.2.1396295264.1552431132; _gcl_au=1.1.404074092.1552323525;
_fbp=fb.1.1552323526191.52071667;CustomCookie=WebInspect141622ZXE000CE7833EE4CBCB1B0690CD295CDC0YC8A5
```

Attack Response:

```
HTTP/1.1 200 OK
Date: Wed, 13 Mar 2019 00:23:29 GMT
X-Frame-Options: SAMEORIGIN
Content-Type: text/html; charset=utf-8
```

```
Content-Length: 16129
ETag: W/"3f01-Sn+DneAOjpxnqwVNVujOl+91Y3U"
Set-Cookie: connect.sid=s%3A2elaWPMp1jpy7vDuK3ggeUpv3kIzZWuL.lbXc8mr31%2FQJ987wrTAX8m2K%
2FKYWnisjECietMsNrjw; Path=/; HttpOnly; Secure
Set-Cookie: ADRUM_BT=R:0|g:070481de-7715-4e9f-bd7f-29b2acf368e95648|s:f|n:PIT_948e56b2-cdee-4f42-bf8d-
46318aebf03f; Path=/; Expires=Wed, 13 Mar 2019 00:23:59 GMT; Secure
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Set-Cookie: BIGipServer~UNIX_Systems~PIT_DDINS-SSL=2711618826.64288.0000; path=/; Httponly; Secure

<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <meta http-equiv="X-UA-Compatible" content="IE=edge" />
    <title>Get A Quote</title>

    <!-- Page-hiding snippet (recommended)  -->
    <style>.async-hide { opacity: 0 !important} </style>
    <script>(function(a,s,y,n,c,h,i,d,e){s.className+=' '+y;h.start=1*new Date;
        h.end=i=function(){s.className=s.className.replace(RegExp(' ?'+y),'')};
        (a[n]=a[n]||[]).hide=h;setTimeout(function(){i();h.end=null},c);h.timeout=c;
    })(window,document.documentElement,'async-hide','dataLayer',4000,
            {'GTM-NPRVDTC':true});</script>
    <!-- Modified Analytics tracking code with Optimize plugin -->
    <script type="text/javascript">
        (function(i, s, o, g, r, a, m) {
            i['GoogleAnalyticsObject'] = r;
            i[r] = i[r] || function() {
                        (i[r].q = i[r].q || []).push(arguments)
                    }, i[r].l = 1 * new Date();
            a = s.createElement(o), m = s.getElementsByTagName(o)[0];
            a.async = 1;
            a.src = g;
            m.parentNode.insertBefore(a, m)
        })(window, document, 'script', '//www.google-analytics.com/analytics.js', 'ga');
        ga('create', 'UA-9398012-1', 'auto');
        ga('require', 'GTM-NPRVDTC', 'auto');
        var dnt= navigator.doNotTrack || window.doNotTrack || window.msDoNotTrack;
        ga('set', 'dimension9', dnt);
        ga('send', 'pageview');
    </script>

        <script type="text/javascript" src="https://maps.googleapis.com/maps/api/js?client=gme-
deltadentalofcalifornia&libraries=places"></script>
        <script type="text/javascript" src="/shopping/js/jquery-8101d596b2.js"></script>

    <script>window['adrum-start-time'] = new Date().getTime();</script>
    <script type="text/javascript" src="/shopping/js/html5shiv-40bd440d29.min.js" async></script>


        <link rel="stylesheet" type="text/css" href="/shopping/styles/style-67c2fc579a.css">


    <link rel="stylesheet" type="text/css" href="//cloud.typography.com/6549574/670548/css/fonts.css" />
</head>
<body>
<!-- MAIN CONTENT -->
              <header class="shopping-header-title">

                                                          <a class="back-arrow-link" id="shoppingBack"
href="https://pit.deltadentalins.com/"><i class="icon  icon-back-arrow-shopping" aria-label="shopping back arrow icon"
><span class="visually-hidden">back to previous page</span></i>
<span class="visually-hidden">back to previous page</span></a>

                                            <div class="main-content">
                                                          <h1 class="shopping-header-content">
                                                                        Get a Quote
                                                          </h1>
                                            </div>
                                            </header>


<main role="main" class="main-content container page-control get-a-quote">
```

```
   <div class="main-container-inner">
     <div class="top-heading-section">
         <div class="error-container global-margin">
         </div>
       <div class="summary grey-text">
         We need a little more information to give you a quote.
       </div>
     </div>
     <form id="get_a_quote" action="/shopping/delta/get-a-quote" method="post">
       <input type="hidden" id="jsEnabled" name="jsEnabled" value="false" />
           <label for="zip"   >What’s your ZIP code?</label>
           <input id="zip"  class="form-input quote_address_zip zip"  type="text" name="zip"  placeholder="ZIP code"      />

           <div class="inline-error-container"

...TRUNCATED...
```

File Names:
- https://pit.deltadentalins.com:443/shopping/delta/get-a-quote?issuerCode=DELTA

Best Practice

Privacy Violation: Autocomplete

Summary:

Most recent browsers have features that will save form field content entered by users and then automatically complete form entry the next time the fields are encountered. This feature is enabled by default and could leak sensitive information since it is stored on the hard drive of the user. The risk of this issue is greatly increased if users are accessing the application from a shared environment. Recommendations include setting autocomplete to "off" on all your forms.

Reference:

Microsoft:
Autocomplete Security

Attack Request:

```
GET /shopping/delta/get-a-quote?issuerCode=DELTA HTTP/1.1
Accept: */*
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64; rv:30.0) Gecko/20100101 Firefox/30.0
Accept-Encoding: gzip, deflate
Host: pit.deltadentalins.com
Connection: Keep-Alive
Pragma: no-cache
Cookie: _ga=GA1.2.1222917316.1517435630; AMCV_E9D70FA75B3A18E80A495C49%40AdobeOrg=1994364360%
7CMCIDTS%7C17967%7CMCMID%7C22137510049759883710112622098244936722%7CMCAAMLH-1552928317%7C9%
7CMCAAMB-1552928317%7CRKhpRz8krg2tLO6pguXWp5olkAcUniQYPHaMWWgdJ3xzPWQmdj0y%7CMCOPTOUT-
1552330717s%7CNONE%7CvVersion%7C3.4.0%7CMCAID%7CNONE%7CMCSYNCSOP%7C411-17946;
_gid=GA1.2.1396295264.1552431132; _gcl_au=1.1.404074092.1552323525;
_fbp=fb.1.1552323526191.52071667;CustomCookie=WebInspect141622ZXE000CE7833EE4CBCB1B0690CD295CDC0YC8A5
```

Attack Response:

```
HTTP/1.1 200 OK
Date: Wed, 13 Mar 2019 00:23:29 GMT
X-Frame-Options: SAMEORIGIN
Content-Type: text/html; charset=utf-8
Content-Length: 16129
ETag: W/"3f01-Sn+DneAOjpxnqwVNVujOl+91Y3U"
Set-Cookie: connect.sid=s%3A2elaWPMp1jpy7vDuK3ggeUpv3kIzZWuL.lbXc8mr31%2FQJ987wrTAX8m2K%
2FKYWnisjECietMsNrjw; Path=/; HttpOnly; Secure
Set-Cookie: ADRUM_BT=R:0|g:070481de-7715-4e9f-bd7f-29b2acf368e95648|s:f|n:PIT_948e56b2-cdee-4f42-bf8d-
46318aebf03f; Path=/; Expires=Wed, 13 Mar 2019 00:23:59 GMT; Secure
Keep-Alive: timeout=5, max=100
```

```
Connection: Keep-Alive
Set-Cookie: BIGipServer~UNIX_Systems~PIT_DDINS-SSL=2711618826.64288.0000; path=/; Httponly; Secure

...TRUNCATED...="zip"   >What's your ZIP code?</label>
        <input id="zip"  class="form-input quote_address_zip zip"  type="text" name="zip"  placeholder="ZIP code"      />

        <div class="inline-error-con...TRUNCATED...  class="hidden"   >Month</label>
             <input id="app0_dob_month"  class="form-input month min_applicant_age"  type="text"
name="app0_dob_month"  placeholder="mm"      maxlength = "2"
                />

             <label for="app0y"  class="hidden"   >day</label>
             <input id="app0_dob_day"  class="form-input day min_applicant_age"  type="text" name="app0_dob_day"
placeholder="dd"      maxlength = "2"
                />

             <label for="app0"  class="hidden"   >Year</label>
             <input id="app0_dob_year"  class="form-input year min_applicant_age"  type="text" name="app0_dob_year"
placeholder="yyyy"      maxlength = "4"
                />


          </field...TRUNCATED... how many people need coverage?</label>
        <input id="noofcovered"  class="form-input quote_add_people noofcovered"  type="text" name="noofcovered"
value="1"     />

        <button  id="minusButton"  t...TRUNCATED...
```

File Names:

- https://pit.deltadentalins.com:443/shopping/delta/get-a-quote?issuerCode=DELTA
- https://pit.deltadentalins.com:443/enroll/delta/payment

Best Practice

Weak Cryptographic Hash

Summary:

A string of hexadecimal digits matching the length of a cryptographic hash from the MD family was detected. Cryptographic hashes are often used to protect passwords, session information, and other sensitive data. There are multiple hashing algorithms in the MD family. By far the most commonly used algorithm is MD5, though MD4 and MD2 are still used with various public key and digital certificate systems. There are known attacks against MD5, MD4, and MD2. These hashes are also susceptible to Rainbow table attacks unless the input is properly salted. As such the MD family of cryptographic hashing functions should not be considered secure and should only be used in certain situations.

Implication:

Hashes produced by the MD family should only be used for short-lived uses where the hash and/or hashed data is not highly security sensitive, or for uses where uniqueness is not a critical requirement. MD Hashes should not be used for any type of long term application such as verifying the integrity of a file or for password storage.

Fix:

For Development:
The application should only use cryptographically secure hashing algorithms, such as SHA-224, SHA-256, SHA-384, or SHA-512. Hashes representing sensitive data should be salted to reduce the effectiveness of rainbow tables.

For Security Operations:
Implement a security policy that precludes the use of MD5, MD4, or MD2 for cryptographic functionality.

For QA:
Make sure that the application is not relying on MD5, MD4, or MD2 for cryptographic functionality.

Reference:

MD5
http://en.wikipedia.org/wiki/MD5
Cryptographic Salting
http://en.wikipedia.org/wiki/Salt_%28cryptography%29

Attack Request:

```
GET /enroll/js/pit-adrum-3725132db5.js HTTP/1.1
Accept: */*
Referer: https://pit.deltadentalins.com/enroll/delta/personal-info
Accept-Language: en-US
```

```
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64; rv:30.0) Gecko/20100101 Firefox/30.0
Accept-Encoding: gzip, deflate
Host: pit.deltadentalins.com
Connection: Keep-Alive
Pragma: no-cache
Cookie: ADRUM_BT=R:83|g:b653ad88-b9ca-41c5-a714-628552112b0d5682|n:PIT_948e56b2-cdee-4f42-bf8d-46318aebf03f;
connect.sid=s%3A2elaWPMp1jpy7vDuK3ggeUpv3kIzZWuL.lbXc8mr31%2FQJ987wrTAX8m2K%2FKYWnisjECietMsNrjw;
BIGipServer~UNIX_Systems~PIT_DDINS-SSL=2711618826.64288.0000; QSI_HistorySession=https%3A%2F%
2Fpit.deltadentalins.com%2Fshopping%2Fdelta%2Fget-a-quote%3FissuerCode%3DDELTA~1552436615256%7Chttps%3A%
2F%2Fpit.deltadentalins.com%2Fshopping%2Fdelta%2Fplan-options%3FissuerCode%3DDELTA~1552436637404%7Chttps%
3A%2F%2Fpit.deltadentalins.com%2Fshopping%2Fdelta%2Fplan-options%2F9801677%3FissuerCode%
3DDELTA~1552436642618; _ga=GA1.2.1222917316.1517435630; AMCV_E9D70FA75B3A18E80A495C49%
40AdobeOrg=1994364360%7CMCIDTS%7C17967%7CMCMID%7C22137510049759883710112622098244936722%
7CMCAAMLH-1552928317%7C9%7CMCAAMB-1552928317%
7CRKhpRz8krg2tLO6pguXWp5olkAcUniQYPHaMWWgdJ3xzPWQmdj0y%7CMCOPTOUT-1552330717s%7CNONE%7CvVersion%
7C3.4.0%7CMCAID%7CNONE%7CMCSYNCSOP%7C411-17946; _gid=GA1.2.1396295264.1552431132; _gat=1;
_gcl_au=1.1.404074092.1552323525; _fbp=fb.1.1552323526191.52071667; ADRUM=s=1552436644875&r=https%3A%2F%
2Fpit.deltadentalins.com%2Fshopping%2Fdelta%2Fplan-options%2F9801677%3F-
1555445888;CustomCookie=WebInspect141622ZXE000CE7833EE4CBCB1B0690CD295CDC0YC8A5
```

Attack Response:

```
HTTP/1.1 200 OK
Date: Wed, 13 Mar 2019 00:24:05 GMT
Server: Apache
X-Frame-Options: SAMEORIGIN
Last-Modified: Fri, 08 Mar 2019 22:53:57 GMT
Accept-Ranges: bytes
Vary: Accept-Encoding
Content-Encoding: gzip
Cache-Control: max-age=86400, public
Content-Length: 37915
Keep-Alive: timeout=5, max=98
Connection: Keep-Alive
Content-Type: application/javascript

;/* Version 28b707b4ae597aaa6317446ec323ad71 v:4.2.8.0,
c:3b331bdb5ca9c18ce583f6d2bad57b4289fa...TRUNCATED...cs.com":"http://cdn.appdynamics.com")+"/adrum-ext.
28b707b4ae597aaa6317446ec323ad71.js";a.adrumXdUrl="https://cdn.appdynamics.com/adrum-xd.
28b707b4ae597aaa6317446ec323ad71.html";a.agentVer="4.2.8.0";a.sendImageBeacon="fal...TRUNCATED...
```

File Names:

- https://pit.deltadentalins.com:443/enroll/js/pit-adrum-3725132db5.js

Best Practice

Weak Cryptographic Hash

Summary:

A string of hexadecmial digits matching the length of a cryptographic SHA-0 or SHA-1 hash was detected. Cryptographic hashes are often used to protect passwords, session information, and other sensitive data. There are known attacks against SHA-0 and SHA-1. While not broken, SHA-0 and SHA-1 are considered weak. Various organizations, such as NIST in the United States, no longer recommend SHA-0 or SHA-1 and these algorithms should only be used in certain situations.

Implication:

The SHA-0 and SHA-1 cryptographic hashing functions are considered weak. You should consider upgrading to a strong hash unless the hash is used for short-lived uses, where the hash and/or hashed data is not highly security sensitive, or for uses where uniqueness is not a critical requirement.

Fix:

For Development:
Consider upgrading to a secure hashing algorithms, such as SHA-224, SHA-256, SHA-384, or SHA-512. Hashes representing sensitive data that is stored for long periods of time should be salted to reduce the effectiveness of rainbow tables.

For Security Operations:
Implement a security policy that precludes the use of SHA-0 and SHA-1 for cryptographic functionality.

For QA:
Make sure that the application is not relying on SHA-0 and SHA-1 for cryptographic functionality.

Reference:

SHA Hash Functions
http://en.wikipedia.org/wiki/SHA_hash_functions
New Cryptoanalytic Results Against SHA-1
http://www.schneier.com/blog/archives/2005/08/new_cryptanalyt.html
NIST Approved Secure Hashing Algorithms
http://csrc.nist.gov/groups/ST/toolkit/secure_hashing.html
Cryptographic Salting
http://en.wikipedia.org/wiki/Salt_%28cryptography%29

Attack Request:

```
GET /enroll/js/pit-adrum-3725132db5.js HTTP/1.1
Accept: */*
Referer: https://pit.deltadentalins.com/enroll/delta/personal-info
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64; rv:30.0) Gecko/20100101 Firefox/30.0
Accept-Encoding: gzip, deflate
Host: pit.deltadentalins.com
Connection: Keep-Alive
Pragma: no-cache
Cookie: ADRUM_BT=R:83|g:b653ad88-b9ca-41c5-a714-628552112b0d5682|n:PIT_948e56b2-cdee-4f42-bf8d-46318aebf03f;
connect.sid=s%3A2elaWPMp1jpy7vDuK3ggeUpv3kIzZWuL.lbXc8mr31%2FQJ987wrTAX8m2K%2FKYWnisjECietMsNrjw;
BIGipServer~UNIX_Systems~PIT_DDINS-SSL=2711618826.64288.0000; QSI_HistorySession=https%3A%2F%
2Fpit.deltadentalins.com%2Fshopping%2Fdelta%2Fget-a-quote%3FissuerCode%3DDELTA~1552436615256%7Chttps%3A%
2F%2Fpit.deltadentalins.com%2Fshopping%2Fdelta%2Fplan-options%3FissuerCode%3DDELTA~1552436637404%7Chttps%
3A%2F%2Fpit.deltadentalins.com%2Fshopping%2Fdelta%2Fplan-options%2F9801677%3FissuerCode%
3DDELTA~1552436642618; _ga=GA1.2.1222917316.1517435630; AMCV_E9D70FA75B3A18E80A495C49%
40AdobeOrg=1994364360%7CMCIDTS%7C17967%7CMCMID%7C22137510049759883710112622098244936722%
7CMCAAMLH-1552928317%7C9%7CMCAAMB-1552928317%
7CRKhpRz8krg2tLO6pguXWp5olkAcUniQYPHaMWWgdJ3xzPWQmdj0y%7CMCOPTOUT-1552330717s%7CNONE%7CvVersion%
7C3.4.0%7CMCAID%7CNONE%7CMCSYNCSOP%7C411-17946; _gid=GA1.2.1396295264.1552431132; _gat=1;
_gcl_au=1.1.404074092.1552323525; _fbp=fb.1.1552323526191.52071667; ADRUM=s=1552436644875&r=https%3A%2F%
2Fpit.deltadentalins.com%2Fshopping%2Fdelta%2Fplan-options%2F9801677%3F-
1555445888;CustomCookie=WebInspect141622ZXE000CE7833EE4CBCB1B0690CD295CDC0YC8A5
```

Attack Response:

```
HTTP/1.1 200 OK
Date: Wed, 13 Mar 2019 00:24:05 GMT
Server: Apache
X-Frame-Options: SAMEORIGIN
Last-Modified: Fri, 08 Mar 2019 22:53:57 GMT
Accept-Ranges: bytes
Vary: Accept-Encoding
Content-Encoding: gzip
Cache-Control: max-age=86400, public
Content-Length: 37915
Keep-Alive: timeout=5, max=98
Connection: Keep-Alive
Content-Type: application/javascript

ion 28b707b4ae597aaa6317446ec323ad71 v:4.2.8.0, c:3b331bdb5ca9c18ce583f6d2bad57b4289faab2d, b:5824 n:31-
4.2.8.next-build */(function(){new f...TRUNCATED...
```

File Names:

- https://pit.deltadentalins.com:443/enroll/js/pit-adrum-3725132db5.js

Best Practice

Web Server Misconfiguration: Insecure Content-Type Setting

Summary:

The Content-Type HTTP response header or the HTML meta tag provides a mechanism for the server to specify an appropriate character encoding for the response content to be rendered in the web browser. Proper specification of the character encoding through the charset parameter in the Content-Type field reduces the likelihood of misinterpretation of the characters in the response content and ensure reliable rendering of the web page.Failure to ensure enforcement of the desired character encoding could result in client-side attacks like Cross-Site Scripting.

Execution:

Verify the character set specification on every HTTP response. Character sets can be specified in the HTTP header or in an HTML meta tag. In the case of an XML response, the character set can be specified along with the XML Declaration.

Implication:

In the absence of the character set specification, a user-agent might default to a non-standard character set, or could derive an incorrect character set based on certain characters in the response content. In some cases, both these approaches can cause the response to be incorrectly rendered. This may enable other attacks such as Cross-site Scripting.

Fix:

Ensure that a suitable character set is specified for every response generated by the web application. This can be done either by,

- Modifying the code of the web application, which would require all pages to be modified.
- Adding Content-Type header to the server configuration (**recommended**). This ensures that the header is added to all the responses with minimal development effort.

Reference:

DoD Application Security and Development STIG
http://iase.disa.mil/stigs/app_security/app_sec/app_sec.html

UTF-7 encoding used to create XSS attack
http://www.securityfocus.com/archive/1/420001

Attack Request:

```
GET /enroll/locale-based/en/US/client-data.json HTTP/1.1
X-Requested-With: XMLHttpRequest
Accept: */*
Referer: https://pit.deltadentalins.com/enroll/delta/personal-info
Accept-Language: en-US
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64; rv:30.0) Gecko/20100101 Firefox/30.0
Host: pit.deltadentalins.com
Connection: Keep-Alive
Pragma: no-cache
Cookie: ADRUM_BT=R:83|g:b653ad88-b9ca-41c5-a714-628552112b0d5682|n:PIT_948e56b2-cdee-4f42-bf8d-46318aebf03f;
connect.sid=s%3A2elaWPMp1jpy7vDuK3ggeUpv3kIzZWuL.lbXc8mr31%2FQJ987wrTAX8m2K%2FKYWnisjECietMsNrjw;
BIGipServer~UNIX_Systems~PIT_DDINS-SSL=2711618826.64288.0000; QSI_HistorySession=https%3A%2F%
2Fpit.deltadentalins.com%2Fshopping%2Fdelta%2Fget-a-quote%3FissuerCode%3DDELTA~1552436615256%7Chttps%3A%
2F%2Fpit.deltadentalins.com%2Fshopping%2Fdelta%2Fplan-options%3FissuerCode%3DDELTA~1552436637404%7Chttps%
3A%2F%2Fpit.deltadentalins.com%2Fshopping%2Fdelta%2Fplan-options%2F9801677%3FissuerCode%
3DDELTA~1552436642618; _ga=GA1.2.1222917316.1517435630; AMCV_E9D70FA75B3A18E80A495C49%
40AdobeOrg=1994364360%7CMCIDTS%7C17967%7CMCMID%7C22137510049759883710112622098244936722%
7CMCAAMLH-1552928317%7C9%7CMCAAMB-1552928317%
7CRKhpRz8krg2tLO6pguXWp5olkAcUniQYPHaMWWgdJ3xzPWQmdj0y%7CMCOPTOUT-1552330717s%7CNONE%7CvVersion%
7C3.4.0%7CMCAID%7CNONE%7CMCSYNCSOP%7C411-17946; _gid=GA1.2.1396295264.1552431132; _gat=1;
_gcl_au=1.1.404074092.1552323525; _fbp=fb.1.1552323526191.52071667; ADRUM=s=1552436644875&r=https%3A%2F%
2Fpit.deltadentalins.com%2Fshopping%2Fdelta%2Fplan-options%2F9801677%3F-
1555445888;CustomCookie=WebInspect141622ZXE000CE7833EE4CBCB1B0690CD295CDC0YC8A5
```

Attack Response:

```
HTTP/1.1 200 OK
Date: Wed, 13 Mar 2019 00:24:06 GMT
Server: Apache
X-Frame-Options: SAMEORIGIN
Last-Modified: Fri, 08 Mar 2019 22:53:57 GMT
Accept-Ranges: bytes
Content-Length: 4763
Cache-Control: max-age=86400, public
Keep-Alive: timeout=5, max=97
Connection: Keep-Alive
Content-Type: application/json

{           "errors":{
                                    "fnameRequired": "Please ente...TRUNCATED...
```

File Names:

- https://pit.deltadentalins.com:443/enroll/locale-based/en/US/client-data.json

Best Practice **Insecure Transport: Missing Perfect Forward Secrecy**

Summary:

Perfect Forward Secrecy (PFS) assures the secrecy of encrypted communications into the future in case SSL/TLS private key is compromised. PFS is a function of key-exchange protocols used for the establishment of shared secret between the client and the server [1]. On a non-forward secrecy server, both the authentication of the server and the encryption is done using long-term private key. Hence, compromised long-term private key can jeopardize all communications. PFS mitigates this by achieving authentication using a long-term private key and session data encryption using a short-term private key. PFS is commonly achieved using Diffie-Hellman in ephemeral-static mode (DHE) or Elliptic Curve Diffie-Hellman key agreement scheme with ephemeral keys (ECDHE) [2, 3, 4]. For every TLS session established with DHE- or ECDHE- as key exchange algorithm in cipher suite, the server is required to use a new Diffie-Hellman public/private key for the generation of the TLS master secret [8]. The server signs this Diffie-Hellman public key using the long-term private key to guarantee authenticity. The long-term private key is not used for the encryption of session contents. While a stolen ephemeral private key could allow an attacker to decipher encrypted communication, the compromise is confined to the specific session for which the ephemeral key was generated. It is recommended that ephemeral keys are not logged.

WebInspect has determined that pit.deltadentalins.com:443 target server configuration contains following issues:
1. Target server supports ECDHE DHE PFS cipher suites but it also uses 9 other cipher suites which do not support PFS:

- **TLS_RSA_WITH_AES_256_CBC_SHA (0x35)**
- **TLS_RSA_WITH_AES_128_CBC_SHA (0x2f)**
- **TLS_RSA_WITH_CAMELLIA_128_CBC_SHA (0x41)**
- **TLS_RSA_WITH_CAMELLIA_256_CBC_SHA (0x84)**
- **TLS_RSA_WITH_AES_256_CBC_SHA256 (0x3d)**
- **TLS_RSA_WITH_AES_128_CBC_SHA256 (0x3c)**
- **TLS_RSA_WITH_AES_256_GCM_SHA384 (0x9d)**
- **TLS_RSA_WITH_AES_128_GCM_SHA256 (0x9c)**
- **TLS_RSA_WITH_3DES_EDE_CBC_SHA (0xa)**

Execution:

A list of supported ciphers by this server can be obtained by running ServerAnalyzer tool from WebInspect toolkit. Notice the absence of "DHE" and "ECDHE" in the list of supported cipher-suite names.

Implication:

A stolen long-term private key can be used by an attacker to decrypt past intercepted communication putting user data at risk where data is still relevant. This shortcoming in SSL/TLS was accentuated in the wake of Heartbleed [4] vulnerability, a vulnerability in Openssl library[4], that allowed attackers to steal server's private keys among other sensitive data.

Fix:

1. PFS is enabled by turning on Diffie-Hellman Ephemeral (DHE) or Elliptic-Curve-Diffie-Hellman Ephemeral (ECDHE) based cipher suites on the server [2]. e.g.

- For Apache – Modify SSLCipherSuite parameter in server configuration to add ECDHE or DHE key exchange algorithm.
- For nginx – Modify ssl_ciphers in server configuration to add ECDHE or DHE key exchange algorithm.
- For IIS please refer to following knowledge base articles:

- http://msdn.microsoft.com/en-us/library/windows/desktop/aa374757(v=vs.85).aspx
- http://support.microsoft.com/kb/245030

2. Make sure that all other cipher suites which do not provide PFS are disabled on the server.

Reference:

http://en.wikipedia.org/wiki/Forward_secrecy
Dierks, T. and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2", RFC 5246, August 2008.
Rescorla, E., "Diffie-Hellman Key Agreement Method", RFC 2631, June 1999.
Blake-Wilson, S., Bolyard, N., Gupta, V., Hawk, C., and B. Moeller, "Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS)", RFC 4492, May 2006.
http://tools.ietf.org/html/rfc4492
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0160
http://www.openssl.org/
http://en.wikipedia.org/wiki/Diffie–Hellman_key_exchange
http://nginx.org/en/docs/http/ngx_http_ssl_module.html
http://httpd.apache.org/docs/2.2/mod/mod_ssl.html

Attack Request:

```
GET /shopping/delta/get-a-quote?issuerCode=DELTA HTTP/1.1
Accept: */*
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64; rv:30.0) Gecko/20100101 Firefox/30.0
Accept-Encoding: gzip, deflate
Host: pit.deltadentalins.com
Connection: Keep-Alive
Pragma: no-cache
Cookie: _ga=GA1.2.1222917316.1517435630; AMCV_E9D70FA75B3A18E80A495C49%40AdobeOrg=1994364360%
7CMCIDTS%7C17967%7CMCMID%7C22137510049759883710112622098244936722%7CMCAAMLH-1552928317%7C9%
7CMCAAMB-1552928317%7CRKhpRz8krg2tLO6pguXWp5olkAcUniQYPHaMWWgdJ3xzPWQmdj0y%7CMCOPTOUT-
1552330717s%7CNONE%7CvVersion%7C3.4.0%7CMCAID%7CNONE%7CMCSYNCSOP%7C411-17946;
_gid=GA1.2.1396295264.1552431132; _gcl_au=1.1.404074092.1552323525;
```

```
_fbp=fb.1.1552323526191.52071667;CustomCookie=WebInspect141622ZXE000CE7833EE4CBCB1B0690CD295CDC0YC8A5
```

Attack Response:

```
HTTP/1.1 200 OK
Date: Wed, 13 Mar 2019 00:23:29 GMT
X-Frame-Options: SAMEORIGIN
Content-Type: text/html; charset=utf-8
Content-Length: 16129
ETag: W/"3f01-Sn+DneAOjpxnqwVNVujOl+91Y3U"
Set-Cookie: connect.sid=s%3A2elaWPMp1jpy7vDuK3ggeUpv3kIzZWuL.lbXc8mr31%2FQJ987wrTAX8m2K%
2FKYWnisjECietMsNrjw; Path=/; HttpOnly; Secure
Set-Cookie: ADRUM_BT=R:0|g:070481de-7715-4e9f-bd7f-29b2acf368e95648|s:f|n:PIT_948e56b2-cdee-4f42-bf8d-
46318aebf03f; Path=/; Expires=Wed, 13 Mar 2019 00:23:59 GMT; Secure
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Set-Cookie: BIGipServer~UNIX_Systems~PIT_DDINS-SSL=2711618826.64288.0000; path=/; Httponly; Secure

<!DOCTYPE html>
<html lang="en">
<head>
  <meta charset="UTF-8">
  <meta name="viewport" content="width=device-width, initial-scale=1.0">
  <meta http-equiv="X-UA-Compatible" content="IE=edge" />
  <title>Get A Quote</title>

  <!-- Page-hiding snippet (recommended)  -->
  <style>.async-hide { opacity: 0 !important} </style>
  <script>(function(a,s,y,n,c,h,i,d,e){s.className+=' '+y;h.start=1*new Date;
    h.end=i=function(){s.className=s.className.replace(RegExp(' ?'+y),'')};
    (a[n]=a[n]||[]).hide=h;setTimeout(function(){i();h.end=null},c);h.timeout=c;
  })(window,document.documentElement,'async-hide','dataLayer',4000,
      {'GTM-NPRVDTC':true});</script>
  <!-- Modified Analytics tracking code with Optimize plugin -->
  <script type="text/javascript">
    (function(i, s, o, g, r, a, m) {
      i['GoogleAnalyticsObject'] = r;
      i[r] = i[r] || function() {
            (i[r].q = i[r].q || []).push(arguments)
          }, i[r].l = 1 * new Date();
      a = s.createElement(o), m = s.getElementsByTagName(o)[0];
      a.async = 1;
      a.src = g;
      m.parentNode.insertBefore(a, m)
    })(window, document, 'script', '//www.google-analytics.com/analytics.js', 'ga');
    ga('create', 'UA-9398012-1', 'auto');
    ga('require', 'GTM-NPRVDTC', 'auto');
    var dnt= navigator.doNotTrack || window.doNotTrack || window.msDoNotTrack;
    ga('set', 'dimension9', dnt);
    ga('send', 'pageview');
  </script>

    <script type="text/javascript" src="https://maps.googleapis.com/maps/api/js?client=gme-
deltadentalofcalifornia&libraries=places"></script>
    <script type="text/javascript" src="/shopping/js/jquery-8101d596b2.js"></script>

  <script>window['adrum-start-time'] = new Date().getTime();</script>
  <script type="text/javascript" src="/shopping/js/html5shiv-40bd440d29.min.js" async></script>


    <link rel="stylesheet" type="text/css" href="/shopping/styles/style-67c2fc579a.css">


  <link rel="stylesheet" type="text/css" href="//cloud.typography.com/6549574/670548/css/fonts.css" />
</head>
<body>
<!-- MAIN CONTENT -->
       <header class="shopping-header-title">

                                            <a class="back-arrow-link" id="shoppingBack"
href="https://pit.deltadentalins.com/"><i class="icon  icon-back-arrow-shopping" aria-label="shopping back arrow icon"
><span class="visually-hidden">back to previous page</span></i>
<span class="visually-hidden">back to previous page</span></a>
```

```
                      <div class="main-content">
                             <h1 class="shopping-header-content">
                                    Get a Quote
                             </h1>
                      </div>
                      </header>


<main role="main" class="main-content container page-control get-a-quote">
 <div class="main-container-inner">
  <div class="top-heading-section">
    <div class="error-container global-margin">
    </div>
   <div class="summary grey-text">
    We need a little more information to give you a quote.
   </div>
  </div>
  <form id="get_a_quote" action="/shopping/delta/get-a-quote" method="post">
   <input type="hidden" id="jsEnabled" name="jsEnabled" value="false" />
     <label for="zip"   >What’s your ZIP code?</label>
     <input id="zip"  class="form-input quote_address_zip zip"  type="text" name="zip"  placeholder="ZIP code"      />

     <div class="inline-error-container"

...TRUNCATED...
```

File Names:

- https://pit.deltadentalins.com:443/shopping/delta/get-a-quote?issuerCode=DELTA