Third party mededeling

Vertrouwelijk

Klant	
Product	AFAS Outsite / Payroll Cloud
Versie	1.0
Auteur	David van der Sluis
Datum	26 juni 2017

Computest

1. Introductie

Op verzoek van verstrekt Computest hierbij een Third Party Mededeling (TPM). Onderwerp van de TPM is de security test die Computest op verzoek van in juni 2017 heeft uitgevoerd op de Outsite en Payroll Cloud omgevingen.

2. Aanpak en scope

Computest heeft een security test uitgevoerd aan de hand van de volgende checklists van Certified Secure:

- Certified Secure Web Application Security Test Checklist v4.2
- Certified Secure Server Security Test Checklist v4.2

Tijdens een dergelijke security test wordt de applicatie door een ethical hacker handmatig getest met ondersteuning van tools. De tester zorgt dat aan het einde van de test ieder item op bovengenoemde checklists gecontroleerd is. Hierdoor ontstaat een transparante en reproduceerbare test.

De rapportage bevat het resultaat van iedere check. Wanneer een checklist-item gefaald is, wordt uitgelegd op welke wijze de kwetsbaarheid zich voordoet, wat de impact is, en hoe deze kwetsbaarheid opgelost kan worden. Aan iedere kwetsbaarheid wordt bovendien een impact-score meegegeven die bepaald is volgens het Common Vulnerability Scoring System (CVSS), versie 2. Deze score duidt de technische impact van de kwetsbaarheid op de vertrouwelijkheid, integriteit en beschikbaarheid van gegevens in het systeem.

Onderwerp van deze test was de Outsite en Payroll Cloud omgevingen.

Deze test is uitgevoerd op de volgende URL's:

- https://beta.afasonline.com/
- https://beta.afasonline.com/payrollcloud/

Deze test is uitgevoerd op het volgende systeem:

beta.afasonline.com

De applicatie is getest vanuit de volgende gebruikersrollen:

- Gebruiker
- Bezoeker

3. Samenvatting resultaten

Tijdens de test zijn 4 kwetsbaarheden aangetroffen, met de volgende CVSS(v2) scores:

CVSS(v2) score			
4.0	2.6	2.6	2.1

Deze kwetsbaarheden betreffen zogeheten “defense in depth”-maatregelen: deze kwetsbaarheden kunnen zelfstandig niet misbruikt worden, maar kunnen door een aanvaller worden gecombineerd om gegevens te stelen of te manipuleren. Het platform zelf is goed beschermd tegen aanvallen vanaf het externe internet.

Computest is gezien de aangetroffen kwetsbaarheden van mening dat de beveiliging van de Outsite en Payroll Cloud omgevingen voldoende is.

4. Checklists

Het doel van deze security test is te bepalen in hoeverre de systemen binnen de scope van deze test kwetsbaar zijn voor een aanval vanaf het internet. De test wordt uitgevoerd aan de hand van de Certified Secure Server Security Test Checklist en de Certified Secure Web Application Security Test Checklist.

#	Certified Secure Server Security Test Checklist	Result	Ref
1.0	**Version Management**		
1.1	Test all services for missing security updates	✓	
1.2	Test all services for unsupported or end-of-life software versions	✓	
2.0	**Network Security**		
2.1	Test for extraneous services	✓	
2.2	Test for extraneous ICMP functionality	✓	
2.3	Test for extraneous enabled network protocols	✓	
2.4	Test for firewall evasion using common techniques	✓	
3.0	**Authentication and Authorization**		
3.1	Test all services for missing authentication or authorization	✓	
3.2	Test all services for predictable credentials	✓	
3.3	Test all services for default, test, guest and obsolete accounts	✓	
3.4	Test all services for missing rate limiting on authentication functionality	✓	
4.0	**Privacy and Confidentiality**		
4.1	Test all services for disclosure of extraneous information	✓	
4.2	Test all services for insecure transmission of sensitive information	✓	
4.3	Test all services for weak, untrusted or expired SSL certificates	✓	
4.4	Test all services for known vulnerabilities in SSL/TLS	✓	
4.5	Test all services for the usage of unproven cryptographic primitives	✓	
4.6	Test all services for incorrect usage of cryptographic primitives	✓	
4.7	Test for publicly accessible test, development and acceptance systems	✓	
4.8	Test for production data stored on non-production systems	✓	
5.0	**Service Specific**		
5.1	Test web services using the Web Application Security Test Checklist	✓	
5.2	Test mail services for open relaying	■	
5.3	Test mail services for e-mail address enumeration	■	
5.4	Test FTP services for anonymous file uploading	■	

#	Certified Secure Server Security Test Checklist	Result	Ref
5.5	Test DNS services for unauthorized AXFR transfers	✓	
6.0	**Miscellaneous**		
6.1	Test for missing rate limiting on resource intensive functionality	✓	
6.2	Test for inappropriate rate limiting resulting in a denial of service	✓	
6.3	Test all services for service-specific issues	✓	
6.4	Test for server- or setup-specific problems	✓	

#	Certified Secure Web Application Security Test Checklist	Result	Ref
1.0	**Deployment**		
1.1	Test for missing security updates	✗	
1.2	Test for unsupported or end-of-life software versions	✓	
1.3	Test for HTTP TRACK and TRACE methods	✓	
1.4	Test for extraneous functionality	✓	
1.5	Test the server using the Server Security Test Checklist	✓	
2.0	**Information Disclosure**		
2.1	Test for extraneous files in the document root	✓	
2.2	Test for extraneous directory listings	✓	
2.3	Test for accessible debug functionality	✓	
2.4	Test for sensitive information in log and error messages	✓	
2.5	Test for sensitive information in robots.txt	■	
2.6	Test for sensitive information in source code	✓	
2.7	Test for disclosure of internal addresses	✓	
3.0	**Privacy and Confidentiality**		
3.1	Test for sensitive information stored in URLs	✓	
3.2	Test for unencrypted sensitive information stored at the client-side	✓	
3.3	Test for sensitive information stored in (externally) archived pages	✓	
3.4	Test for content included from untrusted sources	✓	
3.5	Test for caching of pages with sensitive information	✗	
3.6	Test for insecure transmission of sensitive information	✓	
3.7	Test for non-SSL/TLS pages on sites processing sensitive information	✓	
3.8	Test for SSL/TLS pages served with mixed content	✓	

#	Certified Secure Web Application Security Test Checklist	Result	Ref
3.9	Test for missing HSTS header on full SSL sites	✓	
3.10	Test for known vulnerabilities in SSL/TLS	✓	
3.11	Test for weak, untrusted or expired SSL certificates	✓	
3.12	Test for the usage of unproven cryptographic algorithms	✓	
3.13	Test for the incorrect usage of cryptographic primitives	✓	
4.0	**State Management**		
4.1	Test for client-side state management	✓	
4.2	Test for invalid state transitions	✓	
5.0	**Authentication and Authorization**		
5.1	Test for missing authentication or authorization	✓	
5.2	Test for client-side authentication	✓	
5.3	Test for predictable and default credentials	✓	
5.4	Test for predictable authentication or authorization tokens	✓	
5.5	Test for authentication or authorization based on obscurity	✓	
5.6	Test for identifier-based authorization	✓	
5.7	Test for acceptance of weak passwords	✓	
5.8	Test for plaintext retrieval of passwords	✓	
5.9	Test for missing rate limiting on authentication functionality	✓	
5.10	Test for missing re-authentication when changing credentials	✓	
5.11	Test for missing logout functionality	✓	
6.0	**User Input**		
6.1	Test for SQL injection	✓	
6.2	Test for path traversal and filename injection	✓	
6.3	Test for cross-site scripting	✓	
6.4	Test for system command injection	✓	
6.5	Test for XML injection	✓	
6.6	Test for XPath injection	✓	
6.7	Test for XSL(T) injection	✓	
6.8	Test for SSI injection	✓	
6.9	Test for HTTP header injection	✓	
6.10	Test for HTTP parameter injection	✓	

#	Certified Secure Web Application Security Test Checklist	Result	Ref
6.11	Test for LDAP injection	✓	
6.12	Test for dynamic scripting injection	✓	
6.13	Test for regular expression injection	✓	
6.14	Test for data property/field injection	✓	
6.15	Test for protocol-specific injection	✓	
6.16	Test for expression language injection	✓	
7.0	**Sessions**		
7.1	Test for cross-site request forgery (CSRF)	✓	
7.2	Test for predictable CSRF tokens	✓	
7.3	Test for missing session revocation on logout	✓	
7.4	Test for missing session regeneration on login	✓	
7.5	Test for missing session regeneration when changing credentials	✓	
7.6	Test for missing revocation of other sessions when changing credentials	✓	
7.7	Test for missing Secure flag on session cookies	✓	
7.8	Test for missing HttpOnly flag on session cookies	✓	
7.9	Test for non-restrictive domain on session cookies	✓	
7.10	Test for non-restrictive or missing path on session cookies	✓	
7.11	Test for predictable session identifiers	✓	
7.12	Test for session identifier collisions	✓	
7.13	Test for session fixation	✓	
7.14	Test for insecure transmission of session identifiers	✓	
7.15	Test for external session hijacking	✓	
7.16	Test for missing periodic expiration of sessions	✓	
8.0	**File Uploads**		
8.1	Test for storage of uploaded files in the document root	✓	
8.2	Test for execution or interpretation of uploaded files	✓	
8.3	Test for uploading outside of designated upload directory	✓	
8.4	Test for missing size restrictions on uploaded files	✓	
8.5	Test for missing type validation on uploaded files	✓	
9.0	**Content**		
9.1	Test for missing or non-specific content type definitions	✓	

#	Certified Secure Web Application Security Test Checklist	Result	Ref
9.2	Test for missing character set definitions	✓	
9.3	Test for missing anti content sniffing measures	✗	
10.0	**XML Processing**		
10.1	Test for XML external entity expansion	✓	
10.2	Test for external DTD parsing	✓	
10.3	Test for extraneous or dangerous XML extensions	✓	
10.4	Test for recursive entity expansion	✓	
11.0	**Miscellaneous**		
11.1	Test for missing anti-clickjacking measures	✓	
11.2	Test for open redirection	✗	
11.3	Test for insecure cross-domain access policy	■	
11.4	Test for missing rate limiting on e-mail functionality	✓	
11.5	Test for missing rate limiting on resource intensive functionality	✓	
11.6	Test for inappropriate rate limiting resulting in a denial of service	✓	
11.7	Test for application- or setup-specific problems	✓	