Smart Skills

Your Security Is Our Priority

Rapport Annexe Technique B Partie Serveurs

Version 1.0

Ministère des Domaines de l'État et des Affaires Foncières - 2023

وزارة أملاك الدولة
والشؤون العقارية

i. Détails des Vulnérabilités détectées

I. Injection de demande de connecteur Apache Tomcat AJP (Ghostcat)

ID de Plugin	**134862**	**RISQUE**	Critical	**CVSS score**	9.8
Synopsis	Il existe un connecteur AJP vulnérable en écoute sur l'hôte distant.				
ÉLÉMENTS IMPACTÉS	172.16.10.22,172.16.10.26,172.16.200.20				
Ports associés	8009				
Exploitable :	**Vrai**	**Par Malware :**	**Vrai**	**Age de la vulnérabilité:**	730 days +
Metasploit	-	**Core Impact**	-	**CANVAS**	-

DESCRIPTION

Une vulnérabilité de lecture/inclusion de fichier a été trouvée dans le connecteur AJP. UN Un attaquant distant et non authentifié pourrait exploiter cette vulnérabilité pourlire les fichiers d'application Web à partir d'un serveur vulnérable. Dans les cas oùle serveur vulnérable autorise les téléchargements de fichiers, un attaquant pourrait téléchargercode JavaServer Pages (JSP) malveillant dans divers types de fichierset obtenez l'exécution de code à distance (RCE).

Résultats de Plugin

Nessus was able to exploit the issue using the following request :
0x0000: 02 02 00 08 48 54 54 50 2F 31 2E 31 00 00 0F 2F ....HTTP/1.1.../
0x0010: 61 73 64 66 2F 78 78 78 78 78 2E 6A 73 70 00 00 asdf/xxxxx.jsp..
0x0020: 09 6C 6F 63 61 6C 68 6F 73 74 00 FF FF 00 09 6C .localhost.....l0x0030: 6F 63 61 6C 68 6F 73 74 00 00 50 00 00 09 A0 06 ocalhost..P.....
0x0040: 00 0A 6B 65 65 70 2D 61 6C 69 76 65 00 00 0F 41 ..keep-alive...A0x0050: 63 63 65 70 74 2D 4C 61 6E 67 75 61 67 65 00 00 ccept-Language..
0x0060: 0E 65 6E 2D 55 53 2C 65 6E 3B 71 3D 30 2E 35 00 .en-US,en;q=0.5.
0x0070: A0 08 00 01 30 00 00 0F 41 63 63 65 70 74 2D 45 ....0...Accept-E0x0080: 6E 63 6F 64 69 6E 67 00 00 13 67 7A 69 70 2C 20 ncoding...gzip,
0x0090: 64 65 66 6C 61 74 65 2C 20 73 64 63 68 00 00 0D deflate, sdch...
0x00A0: 43 61 63 68 65 2D 43 6F 6E 74 72 6F 6C 00 00 09 Cache-Control...
0x00B0: 6D 61 78 2D 61 67 65 3D 30 00 A0 0E 00 07 4D 6F max-age=0.....Mo0x00C0: 7A 69 6C 6C 61 00 00 19 55 70 67 72 61 64 65 2D zilla...Upgrade-
0x00D0: 49 6E 73 65 63 75 72 65 2D 52 65 71 75 65 73 74 Insecure-Request0x00E0: 73 00 00 01 31 00 A0 01 00 09 74 65 78 74 2F 68 s...1.....text/h0x00F0: 74 6D 6C 00 A0 0B 00 09 6C 6F 63 61 6C 68 6F 73 tml.....localhos0x0100: 74 00 0A 00 21 6A 61 76 61 78 2E 73 65 72 76 6C t...!javax.servl0x0110: 65 74 2E 69 6E 63 6C 75 64 65 2E 72 65 71 75 65 et.include.reque0x0120: 73 74 5F 75 72 69 00 00 01 31 00 0A 00 1F 6A 61 st_uri...1....ja0x0130: 76 61 78 2E 73 65 72 76 6C 65 74 2E 69 6E 63 6C vax.servlet.incl0x0140: 75 64 65 2E 70 61 74 68 5F 69 6E 66 6F 00 00 10 ude.path_info...
0x0150: 2F 57 45 42 2D 49 4E 46 2F 77 65 62 2E 78 6D 6C /WEB-INF/web.xml0x0160: 00 0A

00 22 6A 61 76 61 78 2E 73 65 72 76 6C 65 ..."javax.servle0x0170: 74 2E 69 6E 63 6C 75 64
65 2E 73 65 72 76 6C 65 t.include.servle0x0180: 74 5F 70 61 74 68 00 00 00 00 FF
t_path.....
This produced the following truncated output (limited to 10 lines) :
---------- snip ----------
..<?xml version="1.0" encoding="UTF-8"?>
<!--
Licensed to the Apache Software Foundation (ASF) under one or morecontributor license agreements. See the NOTICE file distributed withthis work for additional information regarding copyright ownership.
The ASF licenses this file to You under the Apache License, Version 2.0(the "License"); you may not use this file except in compliance withthe License. You may obtain a copy of the License athttp://www.apache.org/licenses/LICENSE-2.0[...]
---------- snip ----------

RÉFÉRENCES

http://www.nessus.org/u?8ebe6246
http://www.nessus.org/u?4e287adb
http://www.nessus.org/u?cbc3d54e
https://access.redhat.com/security/cve/CVE-2020-1745
https://access.redhat.com/solutions/4851251
http://www.nessus.org/u?dd218234
http://www.nessus.org/u?dd772531
http://www.nessus.org/u?2a01d6bf
http://www.nessus.org/u?3b5af27e
http://www.nessus.org/u?9dab109f
http://www.nessus.org/u?5eafcf70

RECOMMENDATIONS

Mettez à jour la configuration AJP pour exiger une autorisation et/ou mettez à niveau le serveur Tomcat vers 7.0.100, 8.5.51, 9.0.31 ou version ultérieure.

II. Signature SMB non requise

ID de Plugin	**57608**	**RISQUE**	Medium	**CVSS score**	5.3
Synopsis	La signature n'est pas requise sur le serveur SMB distant.				
ÉLÉMENTS IMPACTÉS	172.16.10.122,172.16.10.123,172.16.10.15,172.16.10.20,172.16.10.21,172.16.10.23,172.16.10.26,172.16.10.29,172.16.10.6,172.16.10.8				
Ports associés	445				
Exploitable :	**Vrai**	**Par Malware :**	-	**Age de la vulnérabilité:**	-
Metasploit	-	**Core Impact**	-	**CANVAS**	-

DESCRIPTION

La signature n'est pas requise sur le serveur SMB distant. Un non authentifié,
un attaquant distant peut exploiter cela pour mener des attaques de l'homme du milieucontre le serveur SMB.

Résultats de Plugin
-
RÉFÉRENCES
http://www.nessus.org/u?df39b8b3 http://technet.microsoft.com/en-us/library/cc731957.aspx http://www.nessus.org/u?74b80723 https://www.samba.org/samba/docs/current/man-html/smb.conf.5.html http://www.nessus.org/u?a3cac4ea
RECOMMENDATIONS
Appliquez la signature des messages dans la configuration de l'hôte. Sous Windows, cecise trouve dans le paramètre de stratégie « Serveur réseau Microsoft : numériquementsigner les communications (toujours) ». Sur Samba, le paramètre s'appelle 'serveursignature'. Voir les liens « voir aussi » pour plus de détails.

III. Apache Tomcat 7.0.x < 7.0.57 Vulnérabilités multiples (POODLE)

ID de Plugin	**81650**	**RISQUE**	High	**CVSS score**	7.3
Synopsis	Le serveur Apache Tomcat distant est affecté par plusieursvulnérabilités.				
ÉLÉMENTS IMPACTÉS	172.16.10.26				
Ports associés	8443				
Exploitable :	**Vrai**	**Par Malware :**	-	**Age de la vulnérabilité:**	730 days +
Metasploit	-	**Core Impact**	-	**CANVAS**	-

DESCRIPTION

Selon son numéro de version auto-déclaré, Apache Tomcatl'écoute du service sur l'hôte distant est 7.0.x antérieur à 7.0.57. C'est,
donc affecté par les vulnérabilités suivantes :
- Une erreur de double libération de mémoire existe dans 'd1_both.c' lié à la gestion des paquets DTLS qui permettent un déni de service attaques. (CVE-2014-3505)
- Une erreur non spécifiée existe dans 'd1_both.c' liée à gérer les messages de prise de contact DTLS qui permettent le refus de attaques de service dues à de grandes quantités de mémoire consommé. (CVE-2014-3506)
- Il existe une erreur de fuite de mémoire dans 'd1_both.c' liée à gérer des paquets DTLS spécialement conçus qui permettent attaques par déni de service. (CVE-2014-3507)
- Une erreur existe dans la fonction 'OBJ_obj2txt' lorsque diverses jolies fonctions d'impression 'X509_name_*' sont utilisé, ce qui entraîne une fuite des données de la pile de processus, ce qui entraîne un divulgation d'information. (CVE-2014-3508)
- Il existe une erreur liée à « l'extension du format de point ec » gestion et clients multithread qui permettent de libérer mémoire à écraser lors d'une reprise de session. (CVE-2014-3509)
- Il existe une erreur de déréférencement de pointeur NULL liée à gestion des suites de chiffrement ECDH anonymes et conçu messages de prise de contact qui permettent des attaques par déni de service contre les clients. (CVE-2014-3510)
- Il existe une erreur liée à la gestion des fichiers fragmentés Messages « ClientHello » qui permettent à un homme du milieu l'attaquant pour forcer l'utilisation de TLS 1.0, quelle que

soit la valeur supérieure les niveaux de protocole étant pris en charge à la fois par le serveur et le client. (CVE-2014-3511) - Des erreurs de dépassement de tampon existent dans 'srp_lib.c' liées à gestion du protocole Secure Remote Password (SRP) paramètres, qui peuvent permettre un déni de service ou avoir autre impact non précisé. (CVE-2014-3512) - Il existe un problème de fuite de mémoire dans 'd1_srtp.c' lié à la gestion des extensions DTLS SRTP et spécialement conçue messages de prise de contact pouvant permettre un déni de service attaques. (CVE-2014-3513) - Il existe une erreur liée à la façon dont SSL 3.0 gère octets de remplissage lors du déchiffrement des messages chiffrés à l'aide chiffrements par blocs en mode de chaînage de blocs de chiffre
Résultats de Plugin
Installed version : 7.0.52 Fixed version : 7.0.57
RÉFÉRENCES
http://tomcat.apache.org/tomcat-7.0-doc/changelog.html https://www.imperialviolet.org/2014/10/14/poodle.html https://www.openssl.org/~bodo/ssl-poodle.pdf https://tools.ietf.org/html/draft-ietf-tls-downgrade-scsv-00
RECOMMENDATIONS
Mettez à jour vers Apache Tomcat version 7.0.57 ou ultérieure.

IV. Certificat SSL signé à l'aide d'un algorithme de hachage faible

ID de Plugin	**35291**	**RISQUE**	High	**CVSS score**	7.5
Synopsis	Un certificat SSL dans la chaîne de certificats a été signé à l'aide d'unalgorithme de hachage faible.				
ÉLÉMENTS IMPACTÉS	172.16.10.15,172.16.10.21,172.16.10.23,172.16.10.26,172.16.10.29,172.16.10.6				
Ports associés	2222,2223,3389,8443				
Exploitable :	**Vrai**	**Par Malware :**	-	**Age de la vulnérabilité:**	730 days +
Metasploit	-	**Core Impact**	-	**CANVAS**	-
DESCRIPTION					
Le service distant utilise une chaîne de certificats SSL signéeen utilisant un algorithme de hachage cryptographiquement faible (par exemple MD2, MD4, MD5, ou SHA1). Ces algorithmes de signature sont connus pour être vulnérables àattaques par collision. Un attaquant peut exploiter cela pour générer un autrecertificat avec la même signature numérique, permettant à un attaquant dese faire passer pour le service concerné. Notez que ce plugin rapporte toutes les chaînes de certificats SSL signées avecSHA-1 qui expire après le 1er janvier 2017 comme étant vulnérable. C'est dansconformément à la suppression progressive par Google de la cryptographie SHA-1algorithme de hachage. Notez que les certificats de la chaîne contenus dans le NessusLa base de données CA (known_CA.inc) a été ignorée.					
Résultats de Plugin					

The following certificates were part of the certificate chain sent bythe remote host, but contain hashes that are considered to be weak.
Subject : CN=SaibeserverSignature Algorithm : SHA-1 With RSA EncryptionValid From : May 09 20:51:17 2023 GMTValid To : Nov 08 20:51:17 2023 GMTRaw PEM certificate :
-----BEGIN CERTIFICATE-----
MIIC2jCCAcKgAwIBAgIQFhbBI6W/W7xJwKkhlo7YozANBgkqhkiG9w0BAQUFADAWMRQwEgYD
VQQDEwtTYWliZXNlcnZlcjAeFw0yMzA1MDkyMDUxMTdaFw0yMzExMDgyMDUxMTdaMBYxFD
ASBgNVBAMTC1NhaWJlc2VydmVyMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEArG
wj+FyX1JqhUEYu15SzM24Z09yOgNf4oeub+K6wVnneRKeyAdTkuPp6Plw8BB8Y0YmPUXKlNAji5
k/
FWZgpCGEMgn5ZAKGYiugUOoHJJAvXn01Qp4B5sCKkDtQRisVEMQKJ3N5E3SZqr5Hy6RoplQMlc
SKpIjiRyN15uSGMlKIePgWjiSKd2W61cn45QqDkDNwanZdJM/Hd6kgl8vgEdb6m86vb1ygVV/
zv9bojOP41PkzPhFJ6UwAgF0RfvnUBTlMxvRz6A12ptC6zpA8hntcV1Ml6+2apQC/
YGUs3wwA0MNHpWlk2Qel4G4y4Xe8A4PMnSD+LxTHkt7vD3INDbQIDAQABoyQwIjATBgNVHS
UEDDAKBggrBgEFBQcDATALBgNVHQ8EBAMCBDAwDQYJKoZIhvcNAQEFBQADggEBAFgdB/
2DOoOjzqdni4hnDbqr9eC5ude1swzTSqcRKcwKdpL+vzMCGlqa/SqpbqFnMi4Wr/s/
twW7hb2I7l4RsMyKpBICAwPdj9iOJh5MCk7MoaXvfezIyHLsBkDevG3A2MkuPSJGLI/
u9X4NLHDMeIJ+CiMk6VmpctA9O1jw0U0Uie7mUsU06B1F4MLnnRhrEypbTyySMkLNksb9/
zt1tjRNXRDLGKh+w/HapFmANsPkzHlU6bE/
AeXcv0O3WqItylrl3fmzl4nI7vj3Om8DbSsbIYaWUU6aBDtxd5ntxB0bMkFHF6xxOO04uUADzOov
WtJqALWa0pX2m5k9c2Wus5Q=
-----END CERTIFICATE-----

RÉFÉRENCES

https://tools.ietf.org/html/rfc3279
http://www.nessus.org/u?9bb87bf2
http://www.nessus.org/u?e120eea1
http://www.nessus.org/u?5d894816
http://www.nessus.org/u?51db68aa
http://www.nessus.org/u?9dc7bfba

RECOMMENDATIONS

Contactez l'autorité de certification pour faire réémettre le certificat SSL.

V. Faiblesse de l'homme du milieu du serveur de protocole de bureau à distance

ID de Plugin	**18405**	**RISQUE**	Medium	**CVSS score**	6.5
Synopsis	Il peut être possible d'accéder à l'hôte distant.				
ÉLÉMENTS IMPACTÉS	172.16.10.21,172.16.10.22,172.16.10.23,172.16.10.26,172.16.10.29,172.16.10.54,172.16.10.6				
Ports associés	3389				
Exploitable :	**Faux**	**Par Malware :**	-	**Age de la vulnérabilité:**	730 days +
Metasploit	-	**Core Impact**	-	**CANVAS**	-

DESCRIPTION

La version distante du serveur Remote Desktop Protocol (TerminalService) est vulnérable à une attaque

de type man-in-the-middle (MiTM). Le RDPle client ne fait aucun effort pour valider l'identité du serveur lorsquemise en place du cryptage. Un attaquant capable d'intercepterle trafic du serveur RDP peut établir le cryptage avec le clientet le serveur sans être détecté. Une attaque MiTM de cette naturepermettre à l'attaquant d'obtenir toute information sensible transmise, y compris les informations d'authentification. Cette faille existe car le serveur RDP stocke un fichier connu publiquement. Clé privée RSA codée en dur. Tout attaquant dans un réseau privilégiél'emplacement peut utiliser la clé pour cette attaque.
Résultats de Plugin
-
RÉFÉRENCES
http://www.nessus.org/u?8033da0d
RECOMMENDATIONS
- Forcer l'utilisation de SSL comme couche de transport pour ce service sipris en charge, ou/et - Sur les systèmes d'exploitation Microsoft Windows, sélectionnez l'option "Autoriser les connexions". uniquement à partir d'ordinateurs exécutant Remote Desktop avec niveau réseauParamètre d'authentification s'il est disponible.

VI. Suites de chiffrement SSL RC4 prises en charge (Bar Mitzvah)

ID de Plugin	**65821**	**RISQUE**	Medium	**CVSS score**	5.9
Synopsis	Le service distant prend en charge l'utilisation du chiffrement RC4.				
ÉLÉMENTS IMPACTÉS	172.16.10.15,172.16.10.21,172.16.10.22,172.16.10.23,172.16.10.26,172.16.10.29,172.16.10.54,172.16.10.6,172.16.10.8				
Ports associés	3389,8443,10000				
Exploitable :	**Faux**	**Par Malware :**	-	**Age de la vulnérabilité:**	730 days +
Metasploit	-	**Core Impact**	-	**CANVAS**	-

DESCRIPTION

L'hôte distant prend en charge l'utilisation de RC4 dans une ou plusieurs suites de chiffrement.
Le chiffre RC4 est défectueux dans sa génération d'un flux pseudo-aléatoired'octets afin qu'une grande variété de petits biais soient introduits dansle flux, réduisant ainsi son caractère aléatoire.
Si le texte brut est chiffré à plusieurs reprises (par exemple, les cookies HTTP) et qu'unl'attaquant est capable d'obtenir de nombreux textes chiffrés (c'est-à-dire des dizaines de millions),
l'attaquant peut être en mesure de dériver le texte en clair.

Résultats de Plugin

List of RC4 cipher suites supported by the remote server :
High Strength Ciphers (>= 112-bit key)

Name	Code	KEX	Auth	Encryption	MAC
ECDHE-RSA-RC4-SHA	0xC0, 0x11	ECDH	RSA	RC4(128)	SHA1
RC4-MD5	0x00, 0x04	RSA	RSA	RC4(128)	MD5
RC4-SHA					

0x00, 0x05 RSA RSA RC4(128) SHA1The fields above are : {Tenable ciphername} {Cipher ID code} Kex={key exchange} Auth={authentication} Encrypt={symmetric encryption method} MAC={message authentication code} {export flag}
RÉFÉRENCES
https://www.rc4nomore.com/ http://www.nessus.org/u?ac7327a0 http://cr.yp.to/talks/2013.03.12/slides.pdf http://www.isg.rhul.ac.uk/tls/ https://www.imperva.com/docs/HII_Attacking_SSL_when_using_RC4.pdf
RECOMMENDATIONS
Reconfigurez l'application concernée, si possible, pour éviter l'utilisation de RC4chiffres. Envisagez d'utiliser TLS 1.2 avec les suites AES-GCM en fonction du navigateuret prise en charge du serveur Web.

VII. Nom de communauté par défaut de l'agent SNMP (public)

ID de Plugin	**41028**	**RISQUE**	High	**CVSS score**	-
Synopsis	Le nom de communauté du serveur SNMP distant peut être deviné.				
ÉLÉMENTS IMPACTÉS	172.16.10.54				
Ports associés	161				
Exploitable :	**Faux**	**Par Malware :**	-	**Age de la vulnérabilité:**	730 days +
Metasploit	-	**Core Impact**	-	**CANVAS**	-

DESCRIPTION
Il est possible d'obtenir le nom de communauté par défaut du distantServeur SNMP. Un attaquant peut utiliser ces informations pour acquérir davantage de connaissances sur lehôte distant, ou pour modifier la configuration du système distant (sila communauté par défaut autorise de telles modifications).
Résultats de Plugin
The remote SNMP server replies to the following default communitystring : public
RÉFÉRENCES
-
RECOMMENDATIONS
Désactivez le service SNMP sur l'hôte distant si vous ne l'utilisez pas. Soit vous filtrez les paquets UDP entrants allant vers ce port, soit vous modifiez lechaîne de communauté par défaut.

VIII. Le niveau de cryptage des services Terminal Server est moyen ou faible

ID de Plugin	**57690**	**RISQUE**	Medium	**CVSS score**	-
Synopsis	L'hôte distant utilise une cryptographie faible.				
ÉLÉMENTS IMPACTÉS	172.16.10.21,172.16.10.23,172.16.10.26,172.16.10.29,172.16.10.6				
Ports associés	3389				
Exploitable :	-	**Par Malware :**	-	**Age de la vulnérabilité:**	-
Metasploit	-	**Core Impact**	-	**CANVAS**	-
DESCRIPTION					
Le service des services Terminal Server distants n'est pas configuré pour utilisercryptographie. L'utilisation d'une cryptographie faible avec ce service peut permettre à un attaquant deécouter plus facilement les communications et obtenir des captures d'écranet/ou frappes au clavier.					
Résultats de Plugin					
The terminal services encryption level is set to : 2. Medium					
RÉFÉRENCES					
-					
RECOMMENDATIONS					
Remplacez le niveau de cryptage RDP par l'un des suivants : 3. Élevé 4. Conforme FIPS					

IX. Certificat SSL avec un mauvais nom d'hôte

ID de Plugin	**45411**	**RISQUE**	Medium	**CVSS score**	5.3
Synopsis	Le certificat SSL de ce service est destiné à un autre hôte.				
ÉLÉMENTS IMPACTÉS	172.16.10.15,172.16.10.26,172.16.10.29,172.16.10.6				
Ports associés	2222,2223,3389,8443				
Exploitable :	-	**Par Malware :**	-	**Age de la vulnérabilité:**	-
Metasploit	-	**Core Impact**	-	**CANVAS**	-
DESCRIPTION					
L'attribut 'commonName' (CN) du certificat SSL présenté pource service est pour une machine différente.					
Résultats de Plugin					
The identities known by Nessus are : 172.16.10.6 172.16.10.6The Common Name in the certificate is : localhost					
RÉFÉRENCES					
-					

RECOMMENDATIONS
Achetez ou générez un certificat SSL approprié pour ce service.

X. Détection mDNS (réseau distant)

ID de Plugin	**12218**	**RISQUE**	Medium	**CVSS score**	-
Synopsis	Il est possible d'obtenir des informations sur l'hôte distant.				
ÉLÉMENTS IMPACTÉS	172.16.200.20				
Ports associés	5353				
Exploitable :	-	**Par Malware :**	-	**Age de la vulnérabilité:**	-
Metasploit	-	**Core Impact**	-	**CANVAS**	-

DESCRIPTION

Le service distant comprend le Bonjour (également connu sous le nom de ZeroConf oumDNS), qui permet à quiconque de découvrir des informations provenant duhôte distant tel que son type de système d'exploitation et sa version exacte, sonle nom d'hôte et la liste des services qu'il exécute.
Ce plugin tente de découvrir le mDNS utilisé par les hôtes qui ne sont pas sur lesegment de réseau sur lequel réside Nessus.

Résultats de Plugin

Nessus was able to extract the following information :
- mDNS hostname : Webservice.local.
- Advertised services :
o Service name : Webservice [00:50:56:bc:5a:c1]._workstation._tcp.local.
Port number : 9 o Service name : Webservice._ssh._tcp.local.
Port number : 22
- CPU type : I686
- OS : LINUX

RÉFÉRENCES

-

RECOMMENDATIONS

Filtrez le trafic entrant sur le port UDP 5353, si vous le souhaitez.

XI. Certificat SSL auto-signé

ID de Plugin	**57582**	**RISQUE**	Medium	**CVSS score**	6.5
Synopsis	La chaîne de certificats SSL de ce service se termine par uncertificat auto-signé.				
ÉLÉMENTS IMPACTÉS	172.16.10.120,172.16.10.121,172.16.10.122,172.16.10.123,172.16.10.15,172.16.10.20,172.16.10.21,172.16.10.22,172.16.10.23,172.16.10.26,172.16.10.29,172.16.10.54,172.16.10.6,172.16.10.8				
Ports associés	3389,8443,10000				
Exploitable :	-	**Par Malware :**	-	**Age de la vulnérabilité:**	-
Metasploit	-	**Core Impact**	-		-

				CANVAS	

DESCRIPTION

La chaîne de certificats X.509 de ce service n'est pas signée par unautorité de certification reconnue. Si l'hôte distant est un hôte publicen production, cela annule l'utilisation de SSL car n'importe qui pourrait l'établirune attaque de l'homme du milieu contre l'hôte distant.
Notez que ce plugin ne vérifie pas les chaînes de certificats qui se terminentdans un certificat qui n'est pas auto-signé, mais qui est signé par unautorité de certification non reconnue.

Résultats de Plugin

The following certificate was found at the top of the certificatechain sent by the remote host, but is self-signed and was notfound in the list of known certificate authorities :
|-Subject : CN=MDEAF-GEST-PARC.domainetat.local

RÉFÉRENCES

-

RECOMMENDATIONS

Achetez ou générez un certificat SSL approprié pour ce service.

XII. Le certificat SSL n'est pas fiable

ID de Plugin	**51192**	**RISQUE**	Medium	**CVSS score**	6.5
Synopsis	Le certificat SSL de ce service n'est pas fiable.				
ÉLÉMENTS IMPACTÉS	172.16.10.120,172.16.10.121,172.16.10.122,172.16.10.123,172.16.10.15,172.16.10.20,172.16.10.21,172.16.10.22,172.16.10.23,172.16.10.26,172.16.10.29,172.16.10.54,172.16.10.6,172.16.10.8				
Ports associés	636,2222,2223,3269,3389,8443,10000				
Exploitable :	-	**Par Malware :**	-	**Age de la vulnérabilité:**	-
Metasploit	-	**Core Impact**	-	**CANVAS**	-

DESCRIPTION

Le certificat X.509 du serveur n'est pas fiable. Cette situation peutse dérouler de trois manières différentes, dans lesquelles la chaîne de confiance peut êtrecassé, comme indiqué ci-dessous :
- Tout d'abord, le sommet de la chaîne de certificats envoyés par le le serveur ne descend peut-être pas d'un public connu autorité de certification. Cela peut se produire soit lorsque le le sommet de la chaîne est un nom non reconnu et auto-signé certificat, ou lorsque des certificats intermédiaires sont il manque ce qui relierait le haut du certificat chaîne à une autorité de certification publique connue.
- Deuxièmement, la chaîne de certificats peut contenir un certificat qui n'est pas valide au moment de l'analyse. Ceci peut se produire soit lorsque l'analyse a lieu avant l'un des les dates « notBefore » du certificat, ou après l'une des les dates « notAfter » du certificat.
- Troisièmement, la chaîne de certificat peut contenir une signature qui ne correspondaient pas aux informations du certificat ou n'a pas pu être vérifié. Les mauvaises signatures peuvent être corrigées par obtenir le certificat avec la mauvaise signature re-signé par son émetteur. Signatures qui n'ont pas pu être vérifiés sont le résultat de l'émetteur du certificat en utilisant un algorithme de signature que Nessus n'utilise pas non plus soutient ou ne reconnaît pas.

Si l'hôte distant est un hôte public en production, toute interruption dula chaîne rend plus difficile pour les utilisateurs de vérifier l'authenticité etidentité du serveur Web. Cela pourrait faciliter la réalisationattaques de l'homme du milieu contre l'hôte distant.
Résultats de Plugin
The following certificate was at the top of the certificatechain sent by the remote host, but it is signed by an unknowncertificate authority : |-Subject : CN=MDEAF-GEST-PARC.domainetat.local|-Issuer : CN=MDEAF-GEST-PARC.domainetat.local
RÉFÉRENCES
https://www.itu.int/rec/T-REC-X.509/en https://en.wikipedia.org/wiki/X.509
RECOMMENDATIONS
Achetez ou générez un certificat SSL approprié pour ce service.

XIII. SNMP 'GETBULK' Réflexion DDoS

ID de Plugin	**76474**	**RISQUE**	Medium	**CVSS score**	-
Synopsis	Le démon SNMP distant est affecté par une vulnérabilité qui permet à unreflétait une attaque par déni de service distribué.				
ÉLÉMENTS IMPACTÉS	172.16.10.54				
Ports associés	161				
Exploitable :	-	**Par Malware :**	-	**Age de la vulnérabilité:**	730 days +
Metasploit	-	**Core Impact**	-	**CANVAS**	-
DESCRIPTION					
Le démon SNMP distant répond avec une grande quantité de données à unRequête 'GETBULK' avec une valeur supérieure à la normale pour'max-répétitions'. Un attaquant distant peut utiliser ce serveur SNMP pourmener une attaque par déni de service distribué réfléchie sur unhôte distant arbitraire.					
Résultats de Plugin					
Nessus was able to determine the SNMP service can be abused in an SNMPReflection DDoS attack : Request size (bytes) : 42 Response size (bytes) : 1325					
RÉFÉRENCES					
http://www.nessus.org/u?8b551b5c					
RECOMMENDATIONS					
Désactivez le service SNMP sur l'hôte distant si vous ne l'utilisez pas. Sinon, restreignez et surveillez l'accès à ce service et envisagezchanger la chaîne de communauté « publique » par défaut.					

XIV. Algorithmes faibles SSH pris en charge

ID de Plugin	**90317**	**RISQUE**	Medium	**CVSS score**	-
Synopsis	Le serveur SSH distant est configuré pour permettre un cryptage faibledes algorithmes				

	ou pas d'algorithme du tout.				
ÉLÉMENTS IMPACTÉS	172.16.200.20				
Ports associés	22				
Exploitable :	-	**Par Malware :**	-	**Age de la vulnérabilité:**	-
Metasploit	-	**Core Impact**	-	**CANVAS**	-
DESCRIPTION					
Nessus a détecté que le serveur SSH distant est configuré pour utiliserle chiffrement de flux Arcfour ou pas de chiffrement du tout. RFC 4253 conseillecontre l'utilisation d'Arcfour en raison d'un problème avec les touches faibles.					
Résultats de Plugin					
The following weak server-to-client encryption algorithms are supported : arcfour arcfour128 arcfour256The following weak client-to-server encryption algorithms are supported : arcfour arcfour128 arcfour256					
RÉFÉRENCES					
https://tools.ietf.org/html/rfc4253#section-6.3					
RECOMMENDATIONS					
Contactez le fournisseur ou consultez la documentation du produit pour supprimer les éléments faibles. chiffres.					

XV. Fichiers par défaut d'Apache Tomcat

ID de Plugin	**12085**	**RISQUE**	Medium	**CVSS score**	5.3
Synopsis	Le serveur Web distant contient des fichiers par défaut.				
ÉLÉMENTS IMPACTÉS	172.16.200.20				
Ports associés	5050				
Exploitable :	-	**Par Malware :**	-	**Age de la vulnérabilité:**	-
Metasploit	-	**Core Impact**	-	**CANVAS**	-
DESCRIPTION					
La page d'erreur par défaut, la page d'index par défaut, les exemples de JSP et/ou les exemples de servlets sont installés sur l'Apache distant. Serveur Tomcat. Ces fichiers doivent être supprimés car ils peuvent aider un attaquant à découvrir des informations sur le Tomcat distant. installer ou héberger lui-même.					
Résultats de Plugin					
The following default files were found : http://172.16.200.20:5050/docs/ http://172.16.200.20:5050/examples/servlets/index.htmlhttp://172.16.200.20:5050/examples/jsp/index.html					

RÉFÉRENCES
http://www.nessus.org/u?4cb3b4dd https://www.owasp.org/index.php/Securing_tomcat
RECOMMENDATIONS
Supprimez la page d'index par défaut et supprimez l'exemple de JSP et les servlets. Suivez les instructions Tomcat ou OWASP pourremplacer ou modifier la page d'erreur par défaut.

XVI. Détection de service Citation du jour (QOTD)

ID de Plugin	**10198**	**RISQUE**	Medium	**CVSS score**	6.5
Synopsis	Le service de devis (qotd) est en cours d'exécution sur cet hôte.				
ÉLÉMENTS IMPACTÉS	172.16.10.23				
Ports associés	17				
Exploitable :	-	**Par Malware :**	-	**Age de la vulnérabilité:**	730 days +
Metasploit	-	**Core Impact**	-	**CANVAS**	-

DESCRIPTION
Un serveur écoute les connexions TCP sur le port TCP 17. Une fois la connexion établieest établi, un court message est envoyé à la connexion (et toutles données reçues sont jetées). Le service ferme la connexionaprès l'envoi du devis. Un autre service de cotation du jour est défini comme un datagramme baséapplication sur UDP. Un serveur écoute les datagrammes UDP sur le port UDP 17. Lorsqu'un datagramme est reçu, un datagramme de réponse est envoyé contenantun devis (les données du datagramme reçu sont ignorées). Une attaque simple est le « pingpong », dont l'adresse IP usurpe un paquet entre deux machines. en cours d'exécution qotd. Cela les amènera à se lancer des personnages, ralentir les machines et saturer le réseau.
Résultats de Plugin
-
RÉFÉRENCES
-
RECOMMENDATIONS
- Sous les systèmes Unix, commentez la ligne 'qotd' dans /etc/inetd.conf et redémarrez le processus inetd - Sous les systèmes Windows, définissez les clés de registre suivantes à 0 : HKLM\Système\CurrentControlSet\Services\SimpTCP\Parameters\EnableTcpQotd HKLM\ System\CurrentControlSet\Services\SimpTCP\Parameters\EnableUdpQotd Lancez ensuite cmd.exe et tapez : arrêt net simptcp démarrage net simptcp Pour redémarrer le service.

XVII. Détection du protocole TLS version 1.0

ID de Plugin	**104743**	**RISQUE**	Medium	**CVSS score**	6.5
Synopsis	Le service distant chiffre le trafic à l'aide d'une ancienne version de TLS.				
ÉLÉMENTS IMPACTÉS	172.16.10.120,172.16.10.121,172.16.10.122,172.16.10.123,172.16.10.20,172.16.10.21,172.16.10.23,172.16.10.26,172.16.10.29,172.16.10.6,172.16.10.8				
Ports associés	636,3269,3389,8443				
Exploitable :	-	**Par Malware :**	-	**Age de la vulnérabilité:**	-
Metasploit	-	**Core Impact**	-	**CANVAS**	-
DESCRIPTION					
Le service distant accepte les connexions chiffrées à l'aide de TLS 1.0. TLS 1.0 a unnombre de défauts de conception cryptographique. Implémentations modernes de TLS 1.0atténuer ces problèmes, mais les versions plus récentes de TLS comme 1.2 et 1.3 sontconçu contre ces défauts et doit être utilisé autant que possible. Depuis le 31 mars 2020, les points de terminaison qui ne sont pas activés pour TLS 1.2et versions ultérieures ne fonctionneront plus correctement avec les principaux navigateurs Web et les principaux fournisseurs. PCI DSS v3.2 exige que TLS 1.0 soit entièrement désactivé d'ici le 30 juin. 2018, sauf pour les terminaux POS POI (et la terminaison SSL/TLSpoints auxquels ils se connectent) qui peuvent être vérifiés comme n'étant passensible à tout exploit connu.					
Résultats de Plugin					
TLSv1 is enabled and the server supports at least one cipher.					
RÉFÉRENCES					
https://tools.ietf.org/html/draft-ietf-tls-oldversions-deprecate-00					
RECOMMENDATIONS					
Activez la prise en charge de TLS 1.2 et 1.3 et désactivez la prise en charge de TLS 1.0.					

XVIII. Les services Terminal Server n'utilisent pas uniquement l'authentification au niveau du réseau (NLA)

ID de Plugin	**58453**	**RISQUE**	Medium	**CVSS score**	4.0
Synopsis	Les services Terminal Server distants n'utilisent pas uniquement l'authentification au niveau du réseau.				
ÉLÉMENTS IMPACTÉS	172.16.10.21,172.16.10.23,172.16.10.26,172.16.10.29,172.16.10.6				
Ports associés	3389				
Exploitable :	-	**Par Malware :**	-	**Age de la vulnérabilité:**	-
Metasploit	-	**Core Impact**	-	**CANVAS**	-
DESCRIPTION					
Les services Terminal Server distants ne sont pas configurés pour utiliser le niveau réseauAuthentification (NLA) uniquement. NLA utilise le support de sécurité des informations d'identificationProtocole du fournisseur (CredSSP) pour effectuer une authentification forte du serveursoit via les mécanismes TLS/SSL ou Kerberos, qui protègent contreattaques de l'homme du					

milieu. En plus d'améliorer l'authentification, NLA aide également à protéger l'ordinateur distant contre les utilisateurs malveillants etlogiciel en complétant l'authentification de l'utilisateur avant un RDP completla connexion est établie.
Résultats de Plugin
Nessus was able to negotiate non-NLA (Network Level Authentication) security.
RÉFÉRENCES
https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc732713(v=ws.11) http://www.nessus.org/u?e2628096
RECOMMENDATIONS
Activez l'authentification au niveau du réseau (NLA) sur le serveur RDP distant. C'estgénéralement effectué dans l'onglet « À distance » des paramètres « Système » sous Windows.

XIX. Détection du service d'écho

ID de Plugin	**10061**	**RISQUE**	Medium	**CVSS score**	6.5
Synopsis	Un service d'écho est en cours d'exécution sur l'hôte distant.				
ÉLÉMENTS IMPACTÉS	172.16.10.23				
Ports associés	7				
Exploitable :	-	**Par Malware :**	-	**Age de la vulnérabilité:**	730 days +
Metasploit	-	**Core Impact**	-	**CANVAS**	-
DESCRIPTION					
L'hôte distant exécute le service « echo ». Ce servicefait écho à toutes les données qui lui sont envoyées. Ce service n'est pas utilisé de nos jours, il est donc fortement conseillé devous le désactivez, car il peut être utilisé par des attaquants pour configurer le déni deattaques de services contre cet hôte.					
Résultats de Plugin					
-					
RÉFÉRENCES					
-					
RECOMMENDATIONS					
Vous trouverez ci-dessous quelques exemples de désactivation du service d'écho sur certains appareils courants. plates-formes, cependant de nombreux services peuvent présenter ce comportement et la liste ci-dessousn'est pas exhaustif. Consultez la documentation du fournisseur pour le service présentant le comportement d'échopour plus d'informations. - Sous les systèmes Unix, commentez la ligne 'echo' dans /etc/inetd.conf et redémarrez le processus inetd. - Sous les systèmes Ubuntu, commentez la ligne 'echo' dans /etc/systemd/system.conf et redémarrez le service systemd.					

- Sous les systèmes Windows, définissez la clé de registre suivante sur 0 : HKLM\Système\CurrentControlSet\Services\SimpTCP\Parameters\EnableTcpEcho HKLM\ System\CurrentControlSet\Services\SimpTCP\Parameters\EnableUdpEchoLancez ensuite cmd.exe et tapez :
arrêt net simptcp démarrage net simptcpPour redémarrer le service.

XX. Suites de chiffrement SSL de force moyenne prises en charge (SWEET32)

ID de Plugin	**42873**	**RISQUE**	High	**CVSS score**	7.5
Synopsis	Le service distant prend en charge l'utilisation de chiffrements SSL de force moyenne.				
ÉLÉMENTS IMPACTÉS	172.16.10.120,172.16.10.121,172.16.10.122,172.16.10.123,172.16.10.15,172.16.10.20,172.16.10.21,172.16.10.22,172.16.10.23,172.16.10.26,172.16.10.29,172.16.10.54,172.16.10.6,172.16.10.8				
Ports associés	636,3269,3389,8443,10000				
Exploitable :	-	**Par Malware :**	-	**Age de la vulnérabilité:**	730 days +
Metasploit	-	**Core Impact**	-	**CANVAS**	-

DESCRIPTION

L'hôte distant prend en charge l'utilisation de chiffrements SSL qui offrent un supportcryptage de force. Nessus considère la force moyenne comme n'importe quel cryptagequi utilise des longueurs de clé d'au moins 64 bits et de moins de 112 bits, ouautre qui utilise la suite de chiffrement 3DES.
Notez qu'il est considérablement plus facile de contourner la force moyennecryptage si l'attaquant se trouve sur le même réseau physique.

Résultats de Plugin

Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

Name	Code	KEX	Auth	Encryption	MAC
DES-CBC3-SHA	0x00, 0x0A	RSA	RSA	3DES-CBC(168)	SHA1The fields above are :

{Tenable ciphername}
{Cipher ID code}
Kex={key exchange}
Auth={authentication}
Encrypt={symmetric encryption method}
MAC={message authentication code}
{export flag}

RÉFÉRENCES

https://www.openssl.org/blog/blog/2016/08/24/sweet32/
https://sweet32.info

RECOMMENDATIONS

Reconfigurez si possible l'application concernée pour éviter l'utilisation dechiffres de force moyenne.

XXI. Détection de serveur Web non prise en charge

ID de Plugin	**34460**	**RISQUE**	Critical	**CVSS score**	10.0
Synopsis	Le serveur Web distant est obsolète/non pris en charge.				
ÉLÉMENTS IMPACTÉS	172.16.10.23				
Ports associés	81,82,83,84,85,86,88,89,90,99,810				
Exploitable :	-	**Par Malware :**	-	**Age de la vulnérabilité:**	-
Metasploit	-	**Core Impact**	-	**CANVAS**	-
DESCRIPTION					
Selon sa version, le serveur web distant est obsolète et aucunplus entretenu par son vendeur ou son fournisseur. Le manque de support implique qu'aucun nouveau correctif de sécurité pour le produitsera libéré par le vendeur. En conséquence, il peut contenir des informations de sécuritévulnérabilités.					
Résultats de Plugin					
Product : Microsoft IIS 7.0 Server response header : Microsoft-IIS/7.0 Support ended : 2020-01-14 Supported versions : Microsoft IIS 8.5 / 8.0 Additional information : http://www.nessus.org/u?d8353958					
RÉFÉRENCES					
-					
RECOMMENDATIONS					
Supprimez le serveur Web s'il n'est plus nécessaire. Sinon, passez à unversion prise en charge si possible ou passez à un autre serveur.					

XXII. Système d'exploitation Windows non pris en charge (à distance)

ID de Plugin	**108797**	**RISQUE**	Critical	**CVSS score**	10.0
Synopsis	Le système d'exploitation ou le service pack distant n'est plus pris en charge.				
ÉLÉMENTS IMPACTÉS	172.16.10.21,172.16.10.23,172.16.10.26,172.16.10.29,172.16.10.6				
Ports associés	0				
Exploitable :	-	**Par Malware :**	-	**Age de la vulnérabilité:**	-
Metasploit	-	**Core Impact**	-	**CANVAS**	-
DESCRIPTION					
La version distante de Microsoft Windows ne dispose pas d'un service packou n'est plus pris en charge. En conséquence, il est susceptible de contenir des éléments de sécuritévulnérabilités.					
Résultats de Plugin					
The following Windows version is installed and not supported: Microsoft Windows Server 2008 Enterprise Service Pack 2					
RÉFÉRENCES					
https://support.microsoft.com/en-us/lifecycle					

RECOMMENDATIONS
Mise à niveau vers un service pack ou un système d'exploitation pris en charge