Nabídka

Sken zranitelností

Pro zákazníka:

Výzkumný ústav meliorací a ochrany půdy, v.v.i.

Žabovřeská 250, 156 27 Praha 5 - Zbraslav

O2 IT Services

O2 IT Services s.r.o., Za Brumlovkou 226/2, 140 00 Praha 4 – Michle

IČO 02819678, www.o2its.cz

1. Krycí list nabídky

Obchodní firma:	**O2 IT Services s.r.o.**
Sídlo: (úplná adresa pro poštovní styk)	Za Brumlovkou 266/2, Michle, 140 00 Praha 4
Právní forma:	Společnost s ručením omezeným
IČO:	02819678
DIČ:	CZ02819678
Datová schránka:	bedfv84
Kontaktní osoba ve věci nabídky:	[redacted]
Telefon:	[redacted]
Email:	[redacted]

TABULKA 1: PŘEHLED ZMĚN V DOKUMENTU

VERZE	DATUM	AUTOR	ROLE	POPIS
01.00	28.05.2020	[redacted]	Project Manager	Vytvořena Nabídka
01.01	19.11.2020	[redacted]	Project Manager	Aktualizace platnosti nabídky

Ochrana informací

2. Obsah

3. Sken zranitelností

Předmětem nabídky je sken zranitelností na serverech zákazníka: Výzkumný ústav meliorací a ochrany půdy, v.v.i. (dále jen zákazník), který provede dodavatel O2 IT Services s.r.o. (dále jen dodavatel).

Sken zranitelností slouží k identifikaci zranitelností a s tím spojených rizik.

Skenování zranitelností bude provedeno z interní sítě zákazníka prostřednictvím zařízení dodavatele.

Zákazník určí, které servery si přeje oskenovat a poskytne dodavateli informaci k čemu servery slouží a jaké aplikace na nich provozuje.

Dodavatel na serverech prostřednictvím skenu zranitelností vyhledá bezpečnostní slabiny, jak z hlediska operačního systému, tak i z pohledu používaných aplikací (porty; služby; SQL; RDP; IIS; atp.). Dále se dodavatel zaměří na identifikaci a posouzení použitých kryptografických protokolů a použitých šifer.

Při skenování nebude provedena invazivní varianta, která způsobuje nadměrné vytížení a případné negativní ovlivnění funkcionality skenovaných serverů.

4. Rozsah skenování

Skenování bude provedeno na serverech zákazníka v přibližném počtu:

- počet serverů dostupných z internetu (pro sken z veřejné sítě): 10
- Počet serverů v interní síti (pro obvyklý sken): 50

5. Výstup ze skenu zranitelností

Výstupem ze skenu zranitelností je souhrnný a detailní report v anglickém jazyce. V detailním reportu budou uvedeny zjištěné bezpečnostní slabiny a návrh jejich nápravných opatření.

K těmto reportům bude sepsáno manažerské shrnutí v češtině.

Nad výsledky skenu zranitelností proběhne 1 - 2 hodinový workshop, při kterém budou se zákazníkem diskutovány výsledky, a při kterém bude vyčleněn prostor pro otázky.

Ukázka detailního reportu k jednomu nálezu zranitelnosti je vložena do přílohy této nabídky.

6. Součinnost zákazníka

Zajištění součinnosti zodpovědných osob (ve věcech technických i smluvních)

Umožnění přístupu na místo realizace a nastavení oprávnění pro zařízení dodavatele, ze kterého bude provedeno skenování zranitelnosti.

7. Termín plnění

Termín zahájení realizace:	po akceptaci závazné objednávky bude vzájemně odsouhlasen termín samotné implementace.

8. Cena

Jednorázová cena za provedení skenu zranitelností,
vyhodnocení a návrh nápravných opatření: **70 000,-Kč bez DPH**

9. Platnost nabídky

Platnost této cenové nabídky je do 20.12.2020.

10. Příloha – ukázka nálezu v detailním reportu

0	0	5	1	26
CRITICAL	HIGH	MEDIUM	LOW	INFO

Scan Information

Start time: Fri Dec 8 15:27:19 2017
End time: Fri Dec 8 15:35:07 2017

Host Information

DNS Name: itsm.o2its.cz
IP: 160.218.11.146
OS: Microsoft Windows Server 2012 R2

Vulnerabilities

11213 - HTTP TRACE / TRACK Methods Allowed

Synopsis

Debugging functions are enabled on the remote web server.

Description

The remote web server supports the TRACE and/or TRACK methods. TRACE and TRACK are HTTP methods that are used to debug web server connections.

See Also

http://www.cgisecurity.com/whitehat-mirror/WH-WhitePaper_XST_ebook.pdf
http://www.apacheweek.com/issues/03-01-24
http://download.oracle.com/sunalerts/1000718.1.html

Solution

Disable these methods. Refer to the plugin output for more information.

Risk Factor

Medium

CVSS Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)

CVSS Temporal Score

4.3 (CVSS2#E:H/RL:OF/RC:C)

References

BID	9506
BID	9561
BID	11604
BID	33374
BID	37995
CVE	CVE-2003-1567
CVE	CVE-2004-2320
CVE	CVE-2010-0386
XREF	OSVDB:877
XREF	OSVDB:3726
XREF	OSVDB:5648
XREF	OSVDB:11408
XREF	OSVDB:50485
XREF	CERT:288308
XREF	CERT:867593
XREF	CWE:16
XREF	CWE:200

Plugin Information:

Published: 2003/01/23, Modified: 2016/11/23

Plugin Output

tcp/443

```
Use the URLScan tool to deny HTTP TRACE requests or to permit only the
methods needed to meet site requirements and policy.

Nessus sent the following TRACE request :

------------------------------ snip ------------------------------
TRACE /Nessus109120339.html HTTP/1.1
Connection: Close
Host: itsm.o2its.cz
Pragma: no-cache
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */*
Accept-Language: en
Accept-Charset: iso-8859-1,*,utf-8
```

```
------------------------------ snip ------------------------------

and received the following response from the remote server :

------------------------------ snip ------------------------------
HTTP/1.1 200 OK
Content-Type: message/http
Server: Microsoft-IIS/8.5
X-Powered-By: ARR/2.5
X-Powered-By: ASP.NET
Date: Fri, 08 Dec 2017 14:33:40 GMT
Content-Length: 647


TRACE /Nessus109120339.html HTTP/1.1
Connection: Keep-Alive
Pragma: no-cache
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */*
Accept-Charset: iso-8859-1,*,utf-8
Accept-Language: en
Host: itsm.o2its.cz
Max-Forwards: 10
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)
X-Original-URL: /Nessus109120339.html
X-Forwarded-For: 194.228.122.246:59660
X-ARR-SSL: 2048|256|C=US, O=DigiCert Inc, OU=www.digicert.com, CN=Thawte TLS RSA CA G1|C=CZ,
 L="Praha 4, Hlavni mesto Praha", O=O2 IT Services s.r.o., OU=Operations, CN=itsm.o2its.cz
X-ARR-LOG-ID: d79eba4a-3b2b-4561-944e-1d0406f30385

------------------------------ snip ------------------------------
```