

## 2.3 Analiza pola Opis CVE

Jak wspomniano w sekcji 2.1, pole opisu we wpisach CVE jest jednym z kluczowych pól indeksów CVE, z uwagi na informacje, jakie powinno przechowywać. Szczególnie istotne są te dotyczące produktu, jego wersji oraz dostawcy danego produktu. Niestety brak odpowiedniego, zaplanowanego formatowania utrudnia ekstrakcję tych danych z opisu. Dodatkowo nie zawsze wpisy CVE są w pełni opisane. W wielu przypadkach podatności zgłaszane są przez podmioty, które nie mają dostępu do wszystkich pożądanых informacji. W dodatku liczba osób redagujących opisy sprawia, że pod uwagę należy brać styl pisanego, różnice w pisowni lub nazewnictwie produktów, wersji i producentów.

Do dalszej, szczegółowej analizy wybrano kilka wpisów CVE dotyczących produktu Internet Explorer firmy Microsoft. Na ich przykładzie można pokazać najbardziej znaczące cechy pola opisu wpisów CVE oraz omówić ich konsekwencje i problemy przy ich automatycznym przetwarzaniu.

Wpisy wyszukano za pomocą bazy danych NVD, z uwagi na możliwość filtrowania wyników wyszukiwania na podstawie producenta i produktu. Już na tym etapie można było zauważyć, że nazewnictwo w różnych wpisach może przybierać odmienne formy. Na Rysunku 1 widać, że zależnie od autora wpisu wybrany produkt może być inaczej nazwany. W tym przypadku nazwy "ie" oraz "internet explorer" oznaczają to samo oprogramowanie.

Na rysunkach 2-5 można zauważyć iż opisy poszczególnych podatności mają podobną, jednak nie identyczną strukturę. W dwóch przypadkach, na rysunkach 2 i 3, wpis zaczyna się od określenia zakresu wpływu podatności na system, następnie podana jest nazwa producenta oraz nazwa produktu. Kolejnym elementem opisu jest wskazanie wersji produktu, w których wykryto daną podatność. W dalszej części opisu następuje wyjaśnienie istoty danej podatności. W opisach znajdujących się na rysunkach 4 oraz 5 pominięto część dotyczącą zakresu wpływu.

Analizując poszczególne opisy można łatwo wywnioskować, że najbardziej różniącym się między poszczególnymi opisami elementem, jest określenie wersji produktu. W niektórych przypadkach opis ogranicza się do podania wersji produktu jako pojedynczej cyfry. W innych jest to doprecyzowane poprzez dopisanie po kropce dodatkowego identyfikatora wersji. Można spotkać również

The image shows a web-based search interface for the National Vulnerability Database (NVD). It features several filter sections: 'Category (CWE)' with a dropdown menu currently set to 'Any.....'; 'CPE Name' with a text input field and a 'Reset CPE Info' button; 'Vendor' with the text 'microsoft'; and 'Product' with a dropdown menu showing a list of products including 'icm\_color\_management\_module', 'ie', 'ie\_for\_macintosh', 'ie\_toolbar', 'iemobile', 'iis', 'index\_server', 'indexing\_service', 'infopath', 'infotech\_storage\_system\_library', 'interdev', 'interix', 'internet\_authentication\_service\_helper\_com\_component', 'internet\_explorer', 'internet\_information\_server', 'internet\_information\_services', 'isa\_server', 'java\_virtual\_machine', 'jet', and 'jscript'. The interface is part of a larger application, as evidenced by a sidebar on the left with links like 'HE', '10', 'Ga', 'W', 'GE', 'NV', and 'News', and a footer area with 'CVSS V2 Calculator'.

Rysunek 1: Wybór filtrów w wyszukiwarce bazy danych NVD

## Description

Cross-domain vulnerability in Microsoft Internet Explorer 6, 6 SP1, 7, and 8 allows user-assisted remote attackers to bypass the Same Origin Policy and conduct cross-site scripting (XSS) attacks via a crafted HTML document in a situation where the client user drags one browser window across another browser window, aka "HTML Element Cross-Domain Vulnerability."

**Source:** MITRE

**Description Last Modified:** 03/31/2010

Rysunek 2: Pole opisu wpisu CVE-2010-0494

## Description

Use-after-free vulnerability in Microsoft Internet Explorer 5.01 SP4, 6, and 6 SP1 allows remote attackers to execute arbitrary code by changing unspecified properties of an HTML object that has an onreadystatechange event handler, aka "HTML Object Memory Corruption Vulnerability."

**Source:** MITRE

**Description Last Modified:** 03/31/2010

Rysunek 3: Pole opisu wpisu CVE-2010-0491

identyfikator wersji oznaczający pakiet, tak zwany Service Pack. W dodatku niektóre opisy zawierają mieszaną tych oznaczeń determinując poszczególne wersje z różną precyzją. Na rysunku 4 jest ukazany również przypadek, w którym podany jest zakres wersji produktu, w których można spotkać daną podatność. Wszystkie wspomniane różnice mogą powodować wysoki stopień trudności automatycznego przetwarzania opisu. Szczególnie biorąc pod uwagę fakt, że w omówionych przypadkach opisy dotyczyły tego samego produktu.

Na zdjęciach 6-9 przedstawiono opisy dotyczące różnych produktów firmy Microsoft. Przeanalizowane zostaną pod kątem różnic w opisach wpisów CVE dotyczących aplikacji wytworzonych i rozwijanych przez tego samego producenta.

Jak można zauważyć struktura opisu została zachowana jak w przypadku Microsoft Internet Explorer. To znaczy, że na początku opisu znajdują się informacje identyfikujące producenta i produkt, następnie podane są wersje produktu, w których występuje dana podatność. Zachowana została również część nazewnictwa poszczególnych wersji. Niektóre produkty mają jednak nowe

## Description

Microsoft Internet Explorer 6 through 9 does not properly handle objects in memory, which allows remote attackers to execute arbitrary code by accessing an object that (1) was not properly initialized or (2) is deleted, aka "Style Object Memory Corruption Vulnerability."

**Source:** MITRE

**Description Last Modified:** 08/10/2011

Rysunek 4: Pole opisu wpisu CVE-2011-1964

### Description

Microsoft Internet Explorer 8 and 9 does not properly handle objects in memory, which allows remote attackers to execute arbitrary code by accessing a deleted object, aka "OnRowsInserted Event Remote Code Execution Vulnerability."

**Source:** MITRE

**Description Last Modified:** 06/12/2012

Rysunek 5: Pole opisu wpisu CVE-2012-1881

### Current Description

Double free vulnerability in Microsoft Outlook 2007 SP3 and 2010 SP1 and SP2 allows remote attackers to execute arbitrary code by including many nested S/MIME certificates in an e-mail message, aka "Message Certificate Vulnerability."

Rysunek 6: Pole opisu wpisu CVE-2013-3870. Produkt: Microsoft Outlook

### Description

Microsoft Excel 2003 SP3, 2007 SP2 and SP3, and 2010 Gold and SP1; Office 2011 for Mac; Excel Viewer; and Office Compatibility Pack SP2 and SP3 do not properly handle memory during the opening of files, which allows remote attackers to execute arbitrary code via a crafted spreadsheet, aka "Excel File Format Memory Corruption Vulnerability."

**Source:** MITRE

**Description Last Modified:** 05/08/2012

Rysunek 7: Pole opisu wpisu CVE-2012-0141. Produkt: Microsoft Excel

### Description

Cross-site scripting (XSS) vulnerability in Microsoft SharePoint Server 2010 SP1 and SP2 and 2013 allows remote attackers to inject arbitrary web script or HTML via a crafted POST request, aka "POST XSS Vulnerability."

**Source:** MITRE

**Description Last Modified:** 09/11/2013

Rysunek 8: Pole opisu wpisu CVE-2013-3180. Produkt: Microsoft SharePoint Server

### Description

Microsoft Communicator 2007 R2, Lync 2010, Lync 2010 Attendee, and Lync Server 2013 do not properly handle objects in memory, which allows remote attackers to execute arbitrary code via an invitation that triggers access to a deleted object, aka "Lync RCE Vulnerability."

**Source:** MITRE

**Description Last Modified:** 05/14/2013

Rysunek 9: Pole opisu wpisu CVE-2013-1302. Produkt: Microsoft Lync

## Current Description

Use-after-free vulnerability in the `HTMLMediaElement::didMoveToNewDocument` function in `core/html/HTMLMediaElement.cpp` in Blink, as used in Google Chrome before 31.0.1650.48, allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving the movement of a media element between documents.

**Source:** MITRE

**Description Last Modified:** 11/13/2013

Rysunek 10: Pole opisu wpisu CVE-2013-6622. Produkt: Google Blink

## Description

Mozilla Network Security Services (NSS) before 3.16.2.1, 3.16.x before 3.16.5, and 3.17.x before 3.17.1, as used in Mozilla Firefox before 32.0.3, Mozilla Firefox ESR 24.x before 24.8.1 and 31.x before 31.1.1, Mozilla Thunderbird before 24.8.1 and 31.x before 31.1.2, Mozilla SeaMonkey before 2.29.1, Google Chrome before 37.0.2062.124 on Windows and OS X, and Google Chrome OS before 37.0.2062.120, does not properly parse ASN.1 values in X.509 certificates, which makes it easier for remote attackers to spoof RSA signatures via a crafted certificate, aka a "signature malleability" issue.

**Source:** MITRE

**Description Last Modified:** 09/25/2014

Rysunek 11: Pole opisu wpisu CVE-2014-1568. Produkt: Mozilla Network Security Services

identyfikatory wersji, którymi jest rok publikacji oraz występujące w opisie produktu Microsoft Excel słowo "Gold". Dodatkowym elementem opisu jest również wyszczególnienie w nim innych produktów, w których występuje opisywana podatność. Analiza rysunków 6-9 pozwala stwierdzić, że w ramach produktów wytwarzanych przez jedną firmę istnieją różnice w nazewnictwie poszczególnych wersji, nie jest ono jednak znacząco bardziej skomplikowane, niż nazewnictwo wersji w ramach jednego produktu.

Na rysunkach 10-13 znajdują się opisy podatności występujących w produktach stworzonych przez różnych producentów. Pozwoli to przeanalizować różnice pomiędzy strukturami opisów zapewnianych przez zróżnicowane środowiska.

Analizując rysunki 10-13 można stwierdzić, że nazewnictwo wersji poszczególnych produktów mogą przybierać zupełnie różne formy. Ale mają

## Description

Multiple stack-based buffer overflows in Aurigma Image Uploader ActiveX control (ImageUploader4.ocx) 4.6.17.0, 4.5.70.0, and 4.5.126.0, and ImageUploader5 5.0.10.0, as used by Facebook PhotoUploader 4.5.57.0, allow remote attackers to execute arbitrary code via long (1) ExtractExif and (2) ExtractIptc properties.

**Source:** MITRE

**Description Last Modified:** 02/07/2008

Rysunek 12: Pole opisu wpisu CVE-2008-0660. Produkt: Aurigma Image Uploader ActiveX

### Description

The Avira Secure Backup (aka com.avira.avirabackup) application 1.2.3 for Android does not verify X.509 certificates from SSL servers, which allows man-in-the-middle attackers to spoof servers and obtain sensitive information via a crafted certificate.

**Source:** MITRE

**Description Last Modified:** 09/08/2014

Rysunek 13: Pole opisu wpisu CVE-2014-5576. Produkt: Avira Secure Backup

również cechy wspólne. Takim łącznikiem jest na przykład stopniowanie oznaczeń pomiędzy poszczególnymi aktualizacjami. Gdy zmiany w danej wersji są niewielkie, zmienia się tylko ostatni człon w oznaczeniu wersji. Jednak gdy zmiany mają większy wpływ na działanie produktu, wówczas zmieniane są wyższe stopnie w nazwie wersji. Wśród różnic natomiast należy wymienić rzędy liczb definiujących kolejne wersje. Rząd ten, w wybranej próbce opisów, waha się od liczb jednocyfrowych, do liczb czterocyfrowych. Odmienna jest też liczba stopni poszczególnych wersji. Co więcej na rysunku 11 spotkać można oznaczenie "3.16.x" obejmujące wszystkie niższe stopniem aktualizacje wersji "3.16". Informacje te potwierdzają złożoność zagadnienia automatycznego dopasowania wersji produktów zainstalowanych w analizowanym przez IBM Big Fix Inventory systemie.