

Prevenção de ataque *zero-day* por meio de vulnerabilidades divulgadas

Alexandre Yuji Kajihara - 1510762

Agenda

- Introdução;
- *Zero-day*;
- Objetivo;
- Motivação;
- Método;
- Resultados esperados;
- Referências.

Introdução

- Crimes cibernéticos;
 - Qualquer objeto pode ser atacado;
 - *Software* pode conter vulnerabilidades;
 - Vulnerabilidades inexploradas ou não;
 - Fornecedores de *software* lançam atualização.

Zero-day

- Surgiu nos anos 80;
- Vulnerabilidades que não foram divulgadas;
 - Podem permanecer desconhecidos por até dois anos.
- Muito difícil de se defender;
- Prevenções (sensores ou defesas cibernéticas, testes de penetração).

Objetivo

- Prevenção de ataques de *zero-day*;
- Organizações possuem bases de informações das vulnerabilidades;
 - *National Vulnerability Database (NVD)*;
 - *Common Vulnerabilities and Exposures (CVE)*;
 - *Listing of Threats & Risk (Symantec)*.

Motivação

- Internet no nosso dia-a-dia;
 - 2003 - 500 milhões de dispositivos conectados à Internet;
 - 2010 - 12 bilhões de dispositivos conectados à Internet;
 - 2020 - 50 bilhões de dispositivos conectados à Internet;
- Aumentar a segurança;
 - 1ª trimestre 2012 - 7.000 *malwares* presente no *Android*.
- Auxílio aos fornecedores de *software*.

Método

- Combinações dos dados extraídos;
- Reprodução das falhas;
- Verificar ataques *zero-day* conhecidos;
- Pesquisar mais sobre as CVE;
- Dados sempre atualizados.

National Vulnerability Database (NVD)

Description

Cross-zone scripting vulnerability in Apple Quicktime 3 to 7.1.3 allows remote user-assisted attackers to execute arbitrary code and list filesystem contents via a QuickTime movie (.MOV) with an HREF Track (HREFTrack) that contains an automatic action tag with a local URI, which is executed in a local zone during preview, as exploited by a MySpace worm.

Source: MITRE **Last Modified:** 01/04/2007

Quick Info

CVE Dictionary Entry: [CVE-2007-0059](#)
Original release date: 01/04/2007
Last revised: 11/15/2008
Source: US-CERT/NIST

Impact

CVSS Severity (version 2.0):

CVSS v2 Base Score: 6.8 MEDIUM

Vector: (AV:N/AC:M/Au:N/C:P/I:P/A:P) (legend)

Impact Subscore: 6.4

Exploitability Subscore: 8.6

CVSS Version 2 Metrics:

Access Vector: Network exploitable - Victim must voluntarily interact with attack mechanism

Access Complexity: Medium

Authentication: Not required to exploit

Impact Type: Provides user account access, Allows partial confidentiality, integrity, and availability violation; Allows unauthorized disclosure of information; Allows disruption of service

Fonte: <https://nvd.nist.gov/vuln/detail/CVE-2007-0059>

Common Vulnerabilities and Exposures (CVE)

```
=====
Name: CVE-1999-0002
Status: Entry
Reference: SGI:19981006-01-I
Reference: URL:ftp://patches.sgi.com/support/free/security/advisories/19981006-01-I
Reference: CERT:CA-98.12.mountd
Reference: CIAC:J-006
Reference: URL:http://www.ciac.org/ciac/bulletins/j-006.shtml
Reference: BID:121
Reference: URL:http://www.securityfocus.com/bid/121
Reference: XF:linux-mountd-bo

Buffer overflow in NFS mountd gives root access to remote attackers,
mostly in Linux systems.
```

Fonte: <http://cve.mitre.org/data/downloads/allitems.txt>

List of Threats & Risk

Discovered: August 19, 2012
Updated: August 20, 2012 7:17:06 AM
Type: Trojan
Infection Length: 42,913 bytes
Systems Affected: Android

Android package file
The Trojan may arrive as a package with the following details:


File name: fa_ap_ero.apk
Package name: fa.lin.ero
Version: 1.0

File name: LL_ap_ken.apk
Package name: ll.ap.ken
Version: 1.0

Permissions
When the Trojan is being installed, it requests permissions to perform the following actions:

- Initiate a phone call without using the Phone UI or requiring confirmation from the user.
- Open network connections.
- Check the phone's current state.
- Read user's contacts data.
- Access information about networks.

Installation
Once installed, the application will display an icon with the Japanese text "Will you win??"



Fonte: https://www.symantec.com/security_response/writeup.jsp?docid=2012-082005-5451-99&tabid=2

Resultado esperados

- Auxiliar os fornecedores.
 - Ser mais uma alternativa para prevenir o ataque *zero-day*;

Referências

Bertucci, D. (2017). Segurança do data center em 2017. Disponível: <http://www.securityreport.com.br/overview/mercado/seguranca-do-data-center-em-2017/>. Acesso: junho/2017.

Bilge, L., Dumitras, T. (2012). Before we knew it. In *Proceedings of the 2012 ACM Conference on Computer and Communications Security*, pp. 833-844.

CERT.br - Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil. (2012). *Cartilha de segurança para Internet*. Disponível: <https://cartilha.cert.br/livro/cartilha-seguranca-internet.pdf>. Acesso: junho/2017.

Egelman, S., Herley, C., Oorschot, P. C. V. (2013). Markets for zero-day exploits: Ethics and implications. In *Proceedings of the 2013 New Security Paradigms Workshop - Nspw'13*, pp. 41-46.

Evans, D. (2011). *The Internet of things: How the next evolution of the internet is changing everything*. Disponível: http://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf. Acesso: junho/2017.

Foti, P., Armin, J., Cremonini, M. (2015). 0-day vulnerabilities and cybercrime. In *Proceedings of the 10th International Conference on Availability, Reliability and Security*, pp. 711-718.

Kaspersky, E. (2012). *Os perigos dos exploits e dias zero e como preveni-los*. Disponível: <https://eugene.kaspersky.com.br/2012/09/17/os-perigos-dos-exploits-e-dias-zero-e-como-preveni-los-2/>. Acesso: junho/2017.

Kumar, P.; Sheth, R. K. (2016). A review on 0-day vulnerability testing in web application. In *Proceedings of the Second International Conference on Information and Communication Technology for Competitive Strategies - ICTCS '16*.

Last, D. (2016). Forecasting zero-day vulnerabilities. In *Proceedings of the 11th Annual Cyber and Information Security Research Conference – CISRC'16*.

Referências

McAfee Inc. (2012). *Relatório da McAfee sobre ameaças: primeiro trimestre de 2012*. Disponível: <https://www.mcafee.com/br/resources/reports/rp-quarterly-threat-q1-2012.pdf>. Acesso: junho/2017.

McCarthy, L. (2004). *Ataques desconhecidos requerem sistemas avançados de aviso*. Disponível: https://www.symantec.com/region/br/enterprisesecurity/content/expert/BR_3899.html. Acesso: junho/2017.

MITRE Corporation. (2017). *Common Vulnerabilities and Exposures*. Disponível: <https://cve.mitre.org/>. Acesso: junho/2017.

National Institute of Standards and Technology (2017). *National Vulnerability Database*. Disponível: <https://nvd.nist.gov/>. Acesso: junho 2017.

Pedrosa, F. (2007). *Introdução aos exploits*. Disponível: <http://www.revista-programar.info/artigos/introducao-aos-exploits/>. Acesso: junho/2017.

Santos, G. M. dos. (2017). *Bases de vulnerabilidades*. Disponível: <http://mecdb3.c3sl.ufpr.br:8080/xmlui/bitstream/handle/123456789/24169/BasesVulnerabilidades-gms15.pdf?sequence=1..> Acesso: junho/2017.

Symantec Corporation. (2017). *A-Z Listing of Threats & Risks*. Disponível: https://www.symantec.com/security_response/landing/azlisting.jsp. Acesso: junho/2017.