

NETASQ

SEISMO



## SKANER WNĘTRZA SIECI

- wykrywanie podatnych na ataki wersji oprogramowania
- zarządzanie ryzykiem w czasie rzeczywistym
- kontrola aplikacji sieciowych w firmie
- wykrywanie luk i podatności na ataki
- sugestie niezbędnych działań

# JAK DZIAŁA SEISMO?

Błędy i luki bezpieczeństwa w aplikacjach są wykorzystywane przez cyberprzestępców do podejmowania niebezpiecznych ataków na infrastrukturę sieci firmowej. SEISMO jest narzędziem pomagającym administratorowi kontrolować i usuwać podatności na ataki w aplikacjach sieciowych działających w firmie. SEISMO to skaner wnętrza sieci wykrywający słabe punkty i potencjalne wrażliwości na ataki będący uzupełnieniem ochrony sieci realizowanej w oparciu o firewall oraz system wykrywania i blokowania włamań.

SEISMO jest pasywnym skanerem, dzięki czemu jego działanie nie ma żadnego wpływa na wydajność samego urządzenia. SEISMO działa każdorazowo, gdy komputer z sieci LAN wygeneruje ruch, który przechodzi przez urządzenie NETASQ. Ruch taki jest sprawdzany przez firewall a następnie przez IPS, dzięki czemu SEISMO uzyskuje informacje, na temat aplikacji, która dany ruch wygenerowała. Następnie SEISMO sprawdza wykrytą aplikację pod kątem wrażliwości na ataki i zagrożenia, które mogą narazić całą sieć.

Analiza dokonywana jest z wykorzystaniem stale aktualizowanych sygnatur w module ASQ. SEISMO skanuje ruch w czasie rzeczywistym dzięki czemu zapewnia ochronę 24/7 bez konieczności pamiętania o uruchomieniu skanowania jak w przypadku korzystania ze skanerów na żądanie. Wykryte luki w systemie są oznaczane według ich ważności – co pozwala administratorowi określić stacje robocze i serwery, które stanowią największe zagrożenie dla sieci.

1 Zakładka prezentująca wszystkie wykryte luki.

2 Zakładka prezentująca wszystkie aplikacje na stacjach roboczych łączące się z siecią.

3 Zakładka prezentująca te aplikacje na stacjach roboczych, wśród których wykryto luki.

4 Liczba stacji, na których wykryto luki.

5 Poziom zagrożenia.

6 Nazwa luki.

Severity	Name	Affected host	Family	Target	Exploit	Solution
Critical	Mozilla Products Multiple URI Handler's Remote Command Execution Vulnerability	2	Web Client	client	Remote	Yes
Critical	Microsoft Windows URI Handler Remote Command Execution Vulnerability	2	Web Client	client	Remote	Yes
Critical	Sun Java Command Execution and Information Disclosure Vulnerabilities	1	Misc	server, client	Remote	Yes
Critical	Mozilla Firefox/SeaMonkey Code Execution and Information Disclosure	2	Web Client	client	Remote	Yes
Critical	Sun Java Runtime Environment Virtual Machine Code Execution Issue	1	Misc	server, client	Remote	Yes
Critical	Microsoft Windows Internet Explorer Request Forgery Issues	2	Web Client	client	Remote	Yes
Critical	Microsoft Windows Internet Explorer Environment Variable Injection Vulnerabilities	1	Misc	server, client	Remote	Yes
Critical	Sun Java Multiple Code Execution and Security Bypass Vulnerabilities	2	Web Client	client	Remote	Yes
Critical	Mozilla Firefox and SeaMonkey Multiple Remote Code Execution Issues	1	Misc	server, client	Remote	Yes
Critical	Mozilla JavaScript Garbage Collector Code Execution Vulnerability	2	Web Client	client	Remote	Yes
Critical	Mozilla Products Code Execution and Injection Vulnerabilities	4	Web Client	client	Remote	Yes
Critical	Mozilla Products Remote Code Execution and Security Bypass Issues	2	Web Client	client	Remote	Yes
Critical	Sun Java JDK and JRE Code Execution and Security Bypass Issues	1	Misc	server, client	Remote	Yes
Critical	Mozilla Products Code Execution and Security Bypass Vulnerabilities	4	Web Client	client	Remote	Yes
Critical	Mozilla Products Code Execution and Security Bypass Vulnerabilities	4	Web Client	client	Remote	Yes
Critical	Mozilla Products Code Execution and Security Bypass Vulnerabilities	5	Web Client	client	Remote	Yes
Critical	Mozilla Products Code Execution and Security Bypass Vulnerabilities	5	Web Client	client	Remote	Yes

**SEISMO PREZENTUJE WYKRYTE LUKI I PODATNOŚCI NA ATAKI WEWNĄTRZ SIECI**  
 W konsoli Real Time Monitor administrator otrzymuje informacje o lukach w systemie, które narażają sieć na ataki. Zagrożenia te są klasyfikowane według stopnia ważności z punktu widzenia bezpieczeństwa sieci.

U450

U1100

U1500

U6000

## INFORMACJA O ZAGROŻENIU Z SUGESTIĄ DZIAŁANIA

Administrator dysponuje przygotowanym przez NETASQ szczegółowym opisem zagrożenia, jakie niesie ze sobą korzystanie z danej wrażliwej aplikacji. Dostępne są linki do stron producentów oprogramowania, które te luki opisują, jak również odwołania do stron niezależnych organizacji śledzących podatności oprogramowania jak np. CVE. Jeśli dostępna jest już nowsza wersja danej aplikacji, w której luka ta została wyeliminowana SEISMO informuje o tym administratora podając mu link do odpowiedniej strony, z której takie poprawki mogą być pobrane.

Jeśli zagrożenie zostało usunięte w nowszej wersji oprogramowania, SEISMO wskazuje link, na który należy kliknąć aby zaktualizować oprogramowanie i wyeliminować lukę w systemie.

### VULNERABILITY

#### Mozilla Firefox "FirefoxURL" URI Handler Registration Code Execution Vulnerability

A vulnerability has been identified in Mozilla Firefox, which could be exploited by attackers to take complete control of an affected system. This issue is caused by a design error within the "FirefoxURL://" URI handler which is registered by the application during the installation process on Windows, which could be exploited by remote attackers to pass malicious arguments to "FirefoxURL://" and execute arbitrary commands with Chrome privileges by tricking a user into visiting a specially crafted web page using Internet Explorer.

Severity

Critical

Detection: Yes

Discovery date: 2007-07-10

Target: Client

Solution: Upgrade to Firefox version 2.0.0.5 : <http://www.mozilla.com/firefox/>

Protecting patterns:

ASQ signature:/alarm name

Available since

Vulnerable versions: Mozilla Firefox version 2.0.0.4 and prior  
Reference:

<http://www.xs-sniper.com/sniperscope/IE-Pwns-Firefox.html>  
<http://marholm.com/2007/07/10/internet-explorer-0day-exploit/>  
<http://www.mozilla.org/security/announce/2007/mfsa2007-23.html>

CVE:  
[CVE-2007-3670](https://cve.mitre.org/cgi-bin/cvebin/cve-2007-3670)

Detected by Seismo beginning with ASQ version 3.5.0

ASQ version of this firewall: 3.5.0

Range:  
Remote

Last update: 2007-10-10

## ELIMINOWANIE PODATNOŚCI NA ATAKI

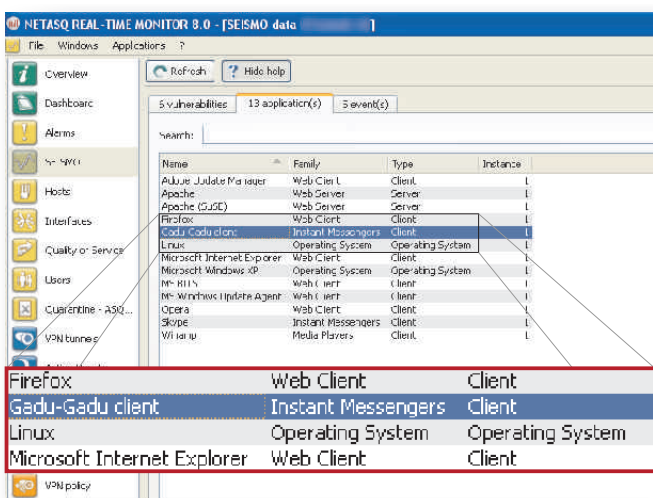
Do każdego wykrytego zagrożenia przygotowany jest opis, podane są linki do strony producenta wrażliwej aplikacji oraz niezależnych organizacji które opisywały daną wrażliwość.

## SEISMO - UNIKATOWE NARZĘDZIE

Urządzenia NETASQ służą do zintegrowanego zabezpieczenia sieci i są jedynymi rozwiązaniami na rynku oferującymi połączenie skanera wnętrza sieci z zaawansowanym systemem intrusion prevention chroniącym przed włamaniami z zewnątrz.

## LISTA PRACUJĄCYCH APLIKACJI SIECIOWYCH

Oprócz wykrywania luk i podatności na ataki, SEISMO dostarcza administratorowi informacje o wrażliwych aplikacjach sieciowych zainstalowanych na komputerach w firmie. Daje to możliwość kontroli czy użytkownicy nie korzystają z aplikacji, z których ze względów bezpieczeństwa korzystać nie powinni.



Name	Family	Type	Instance
Adobe Acrobat Manager	Web Client	Client	L
Apache	Web Server	Server	L
Apache (GUC)	Web Server	Server	L
Firefox	Web Client	Client	L
Gadu-Gadu client	Instant Messengers	Client	L
Linux	Operating System	Operating System	L
Microsoft Internet Explorer	Web Client	Client	L
Microsoft Windows XP	Operating System	Operating System	L
MS-WinSxS	Web Client	Client	L
MS-Windows Update Agent	Web Client	Client	L
Opera	Web Client	Client	L
Skype	Instant Messengers	Client	L
Wii isau	Media Players	Client	L

## BLOKOWANIE WYBRANYCH APLIKACJI NA FIREWALLU LUB IPS

Na podstawie informacji dostarczanych przez SEISMO administrator może na bieżąco podnosić poziom bezpieczeństwa sieci. Wiedząc, że użytkownicy korzystają z aplikacji, które mogą narazić sieć na atak, wyciek informacji (komunikatory internetowe - Gadu-Gadu, Skype, MSN) lub niepotrzebnie obciążają łącze (radia internetowe, P2P) administrator może zdecydować o ustawieniu reguł na firewallu lub IPS, które zablokują taki ruch dla wybranych użytkowników.

## RAPORTOWANIE

Administrator na podstawie informacji, które dostarcza SEISMO może generować okresowe raporty, prezentujące stan bezpieczeństwa całego systemu i stopień jego poprawy na skutek eliminowania wrażliwości wskazanych przez skaner wnętrza sieci.

Po kliknięciu na daną aplikację w bardzo szybki sposób można odnaleźć wszystkie komputery, na których jest ona zainstalowana, sprawdzić dokładną wersję tej aplikacji oraz system operacyjny pod jakim działa ta stacja.

## SEISMO WYKRYWA GADU-GADU I INNE APLIKACJE SIECIOWE

NETASQ SEISMO prezentuje administratorowi szczegółową listę aplikacji sieciowych pracujących na stacjach roboczych jak np. Google Desktop, Firefox, Gadu-Gadu, programy antywirusowe itp.

## INFORMACJE ZBIERANE PRZEZ SEISMO

- luki i podatności w aplikacjach,
- wersje przeglądarek, klientów pocztowych i innych aplikacji sieciowych,
- systemy operacyjne na stacjach roboczych,
- charakterystyka podatności.



[www.netasq.pl](http://www.netasq.pl)



"Décision Informatique", "01 Réseaux"