^ 이전글 ^ 다음글 목록

| 일반 소스 공유 | >

[Rhino] 개선된 세이프 이발(실행) 함수



OnTheWay 챗봇 고수 🏺 1:1 채팅

2019.10.27. 23:13 조회 306

댓글 13 URL 복사 :

[이전 버전입니다! 최신 게시글의 소스를 사용해 주세요!]

최근들어, 안전하게 소스를 실행하는 '세이프 이발' 기능을 많은 카카오톡 봇이 가지고 있습니다. 이 기능은, 카카오톡 봇 어플처럼 직접 Rhino 엔진을 사용하여 자바스크립트 소스를 실행하는 방식을 사용하고 있어요.

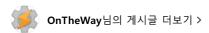
이번에 '세이프 이발' 기능의 중대한 취약점(?)이 발견 되었는데요, 이 취약점은 Rhino의 오류 객체 내부, 'rhinoException' 이라는 자바 클래스를 통하여 다른 클래스에 접근할 수 있는 위험성을 가지고 있습니다.

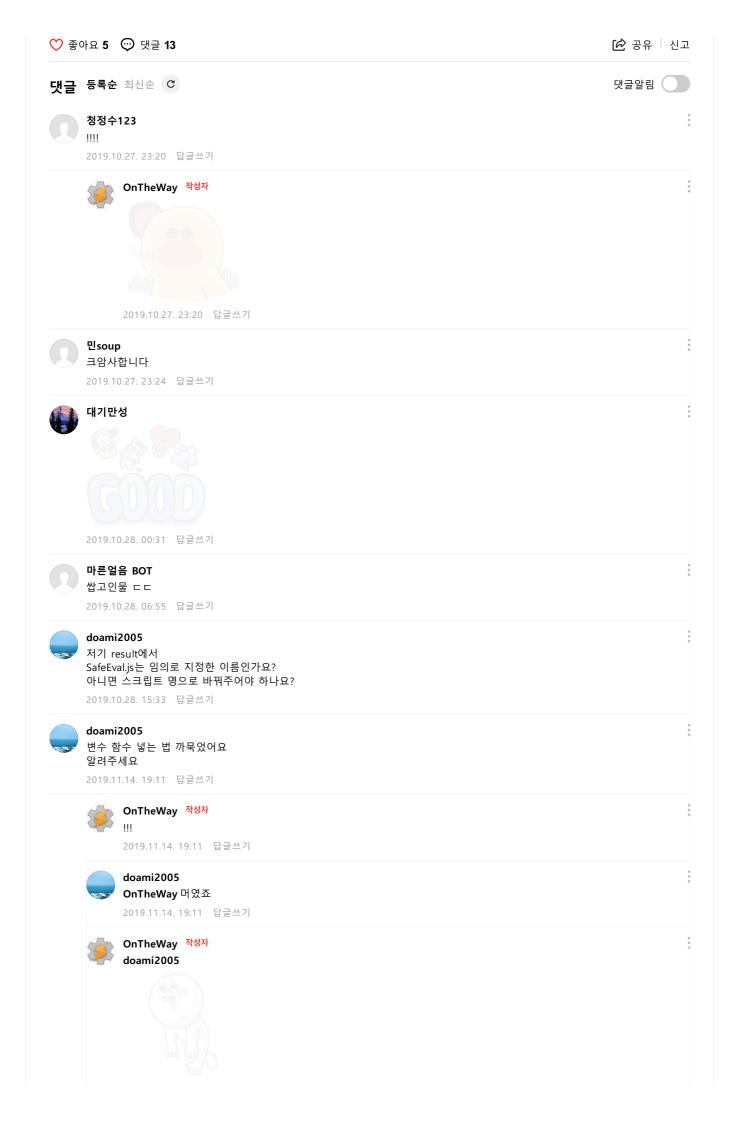
따라서 이번 취약점을 해결할 수 있는, 개선된 '세이프 이발' 함수를 제작하였습니다!

```
[ 소스 ]
```

```
function runSafeEval(src) {
var factory = org.mozilla.javascript.ContextFactory.getGlobal();
var cx = factory.enterContext();
var scope = cx.initSafeStandardObjects();
var result;
cx.setOptimizationLevel(-1);
cx.setInstructionObserverThreshold(3000);
cx.setMaximumInterpreterStackDepth(1000);
cx.getWrapFactory().setJavaPrimitiveWrap(false);
cx.setClassShutter(new org.mozilla.javascript.ClassShutter({
visibleToScripts: function(fullClassName) {
return false;
}
}));
try {
result = cx.evaluateString(scope, src, "SafeEval.js", 1, null);
} catch (err) {
result = err.toString();
}
cx.exit();
return result;
}
[ 사용법 ]
runSafeEval(소스); // 소스 실행 결과를 반환합니다.
___
* Rhino의 'ClassShutter'는 자바 클래스 접근 자체를 방지합니다.
```

많은 분들이 이 소스를 사용해 주셨으면 좋겠네요!







답글 🖍 글쓰기 목록 ▲ TOP

' 일반 소스 공유 ' 게시판 글			0	이 게시판 새글 구독하기		
유사도 함수 🍪 <mark>[21]</mark>					kyleok	2019.10.28.
제이슾 인사봇 [2]					Anseojin	2019.10.28.
[Rhino] 개선된 세이프 이발(실행) 함수 [13]					OnTheWay	2019.10.27.
끝말잇기 [14]					구름	2019.10.27.
2째 Jsoup 날씨 (연습) [13]					Anseojin	2019.10.27.
	1 2	! 3				전체보기

이 카페 인기글



요즘 나타나는 새로운 홍보 수법 중 하나가

Dark Tornado ♥0 ⊕7



틱택토 (Player vs Bot)

도미 doami2005 ♥0 ⊕4

[카카오톡 봇] 양산형 자동학습 봇 소스 공유

Dark Tornado ♥1 ♥5



可以是是数5 AlphaDo ♥3 ♥8 함수를 입력받아 그래프 그리기

y and management of the state o

혹시 여기서 변수를 저장하는 부분이 어딘지

1 2 3 4 5

오픈이발 괴롭히기(메봇R)

● MAS 2만분 환 경기 단체 경기 기 으로 바이번 이 소리 링크를 포함한 글 홍보시 링크 분석(?)하기