Waktu mulai :2018/11/05 13:19:27 - Waktu akhir :2018/11/05 13:19:27

Waktu mulai :2018/11/05 13.26.19 - Waktu akhir :2018/11/05 13.26.19

Waktu mulai :2018/11/05 13.30.28 - Waktu akhir :2018/11/05 13.30.28

Waktu mulai :2018/11/05 13.42.41 - Waktu akhir :2018/11/05 13.42.41

Waktu mulai :2018/11/05 13.45.40 - Waktu akhir :2018/11/05 13.45.40

Waktu mulai :2018/11/05 13.50.31 - Waktu akhir :2018/11/05 13.50.31

Dari IP : 172.30.10.9

Port : 63941

Interface : ethernet0/0

Ke IP : 172.30.10.28

Port : 80

Interface : ethernet0/1

Action : Log Only

Profile : predef\_loose

Signature ID : 305171

URL : [http://172.30.10.28/index.php/category/pets/birds/?method%3A%23\_memberAccess%3D%40ognl.OgnlContext%40DEFAULT\_MEMBER\_ACCESS%2C%2](http://172.30.10.28/index.php/category/pets/birds/?method%3A%23_memberAccess%3D%40ognl.OgnlContext%40DEFAULT_MEMBER_ACCESS%2C%252)

Nama serangan : WEB-SERVER Apache Struts Dynamic Method Invocation Remote Code Execution Vulnerability -3 (CVE-2016-3081)

tipe serangan : web attack

Severity : kritis

Bug ID : 87327

CVE ID : CVE-2016-3081, CVE-2016-3082

Deskripsi :

Apache Struts 2.x sebelum 2.3.20.2, 2.3.24.x sebelum 2.3.24.2, dan 2.3.28.x sebelum 2.3.28.1, ketika Dynamic Method Invocation diaktifkan, memungkinkan penyerang jauh untuk mengeksekusi kode arbitrer melalui metode: awalan, terkait dengan ekspresi dirantai.

Dampak:

Penyerang dapat mengeksekusi kode arbitrer melalui eksploit yang sukses dalam konteks perangkat lunak yang rentan.

Sistem Terpengaruh: Solaris, FreeBSD, Windows, Linux, Lainnya Unix, Mac OS

Referensi Tambahan: SecurityFocusBID: 87327

SecurityFocusBID: 91787

SecurityTrackerID: 1035665

ExploitDB: 39756

Solusi :

Nonaktifkan Perizinan Metode Dinamis bila memungkinkan atau tingkatkan ke Apache Struts versi 2.3.20.3, 2.3.24.3 atau 2.3.28.1.