**Tugas Keamana Jaringan Komputer**

**Disusun Oleh:**

**Aditiya Gunanta**

**09011181520001**

**Universitas Sriwijaya**

**Fakultas Ilmu Komputer**

**Jurusan Sistem Komputer**

**2019**

1. **Target Site**

**https://**[**www.kemenag.go.id**](http://www.kemenag.go.id)

**https://**[**www.rfclassic.lytogame.com**](http://www.rfclassic.lytogame.com)

[**http://www.rf-moonlight.com**](http://www.rf-moonlight.com)

1. **Kementrian Agama Indonesia**

Site Title : Website Kementrian Agama

First date seen : July 2010

Language : Indonesia

Domain : kemenag.go.id

Ip Address : 103.7.15.217

Name Server : dns2.kemenag.go.id

Dns Admin : dns@kemenag.go.id

| **Netblock owner** | **IP address** | **OS** | **Web server** | **Last seen** [Refresh](https://toolbar.netcraft.com/site_report?url=http://kemenag.go.id&refresh=1#history_table) |
| --- | --- | --- | --- | --- |
| [Kementerian Agama KEMENAG Government / Direct Member IDNIC Jl. Lapangan Banteng Barat No.3-4 Jakarta Pusat 10340](https://toolbar.netcraft.com/netblock?q=IDNIC-KEMENAG-ID,103.7.12.0,103.7.15.255)  | 103.7.12.100 | unknown | nginx/1.5.7 | 19-Jun-2016 |
| [Kementerian Agama KEMENAG Government / Direct Member IDNIC Jl. Lapangan Banteng Barat No.3-4 Jakarta Pusat 10340](https://toolbar.netcraft.com/netblock?q=IDNIC-KEMENAG-ID,103.7.12.0,103.7.15.255)  | 103.7.12.72 | Linux | nginx/1.5.7 | 16-Aug-2015 |
| [Kementerian Agama KEMENAG Government / Direct Member IDNIC Jl. Lapangan Banteng Barat No.3-4 Jakarta Pusat 10340](https://toolbar.netcraft.com/netblock?q=IDNIC-KEMENAG-ID,103.7.12.0,103.7.15.255)  | 103.7.12.68 | Linux | nginx/1.5.7 | 28-Jan-2015 |
| [Kementerian Agama KEMENAG Government / Direct Member IDNIC Jl. Lapangan Banteng Barat No.3-4 Jakarta Pusat 10340](https://toolbar.netcraft.com/netblock?q=IDNIC-KEMENAG-ID,103.7.12.0,103.7.15.255)  | 103.7.12.72 | Linux | nginx/1.5.7 | 25-Jun-2014 |
| [Kementerian Agama KEMENAG Government / Direct Member IDNIC Jl. Lapangan Banteng Barat No.3-4 Jakarta Pusat 10340](https://toolbar.netcraft.com/netblock?q=IDNIC-KEMENAG-ID,103.7.12.0,103.7.15.255)  | 103.7.12.72 | Linux | nginx/1.2.6 | 4-Nov-2013 |
| [Kementerian Agama KEMENAG Government / Direct Member IDNIC Jl. Lapangan Banteng Barat No.3-4 Jakarta Pusat 10340](https://toolbar.netcraft.com/netblock?q=IDNIC-KEMENAG-ID,103.7.12.0,103.7.15.255)  | 103.7.12.70 | Linux | Apache/2.2.3 CentOS | 14-Apr-2013 |
| [DEPAG Jakarta Raya](https://toolbar.netcraft.com/netblock?q=LA-D,183.91.84.0,183.91.84.127)  | 183.91.84.5 | Linux | Apache/2.2.3 ClearOS | 18-Nov-2011 |
| [PT Telkom Indonesias customer.](https://toolbar.netcraft.com/netblock?q=TLKM_D2_AST_CUSTOMER,118.97.53.88,118.97.97.95)  | 118.97.64.55 | Linux | Apache/2.2.3 ClearOS | 18-Dec-2010 |

1. **RF Online Classic Indonesia**

Site Title : RF Online Indonesia

First Date Seen : November 2016

Language : Malay

Domain : lytogame.com

Ip Address : 202.93.17.160

Name Server : nama3.thamrin.net.id

Dns admin : admin

| **Netblock owner** | **IP address** | **OS** | **Web server** | **Last seen** [Refresh](https://toolbar.netcraft.com/site_report?url=http://rfclassic.lytogame.com&refresh=1#history_table) |
| --- | --- | --- | --- | --- |
| [PT Lyto Datarindo Fortuna Corporate / Direct Member IDNIC Publisher Game Jakarta](https://toolbar.netcraft.com/netblock?q=IDNIC-LYTO-ID,202.93.16.0,202.93.23.255)  | 202.93.17.160 | unknown | Microsoft-IIS/8.5 | 11-Feb-2019 |

1. **RF Moonlight**

Site Title : RF Moonlight

Fisrt Seen : September 2015

Language : English

Domain : rf-moonlight.com

Ip Address : 212.129..27.167

Name Server : ns10.uadns.com

Dns admin : hostmaster@nic.ua

| **Netblock owner** | **IP address** | **OS** | **Web server** | **Last seen** [Refresh](https://toolbar.netcraft.com/site_report?url=http://www.rf-moonlight.com&refresh=1#history_table) |
| --- | --- | --- | --- | --- |
| [Online SAS - Dedibox](https://toolbar.netcraft.com/netblock?q=Online,212.129.0.0,212.129.31.255)  | 212.129.27.167 | unknown | Microsoft-IIS/10.0 | 11-Feb-2019 |

1. **Web tracing**
2. **Kemenag.go.id**



1. **Rfclassic.lytogame.com**



1. **Rf-moonlight.com**



1. **CVE Vulnerabilities**
2. **Kemenag.go.id**

|  |  |
| --- | --- |
| [CVE-2019-1673](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-1673) | A vulnerability in the web-based management interface of Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web-based interface. The vulnerability is due to insufficient input validation of some parameters passed to the web-based management interface. An attacker could exploit this vulnerability by convincing a user of the interface to click a specific link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the interface or allow the attacker to access sensitive browser-based information. For information about fixed software releases, consult the Cisco bug ID at https://quickview.cloudapps.cisco.com/quickview/bug/CSCvn64652. When considering software upgrades, customers are advised to regularly consult the advisories for Cisco products, which are available from the Cisco Security Advisories and Alerts page, to determine exposure and a complete upgrade solution.  |
| [CVE-2019-1653](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-1653) | A vulnerability in the web-based management interface of Cisco Small Business RV320 and RV325 Dual Gigabit WAN VPN Routers could allow an unauthenticated, remote attacker to retrieve sensitive information. The vulnerability is due to improper access controls for URLs. An attacker could exploit this vulnerability by connecting to an affected device via HTTP or HTTPS and requesting specific URLs. A successful exploit could allow the attacker to download the router configuration or detailed diagnostic information. Cisco has released firmware updates that address this vulnerability.  |

1. **rfclassic.lytogame.com**

|  |  |
| --- | --- |
| [CVE-2019-1673](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-1673) | A vulnerability in the web-based management interface of Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web-based interface. The vulnerability is due to insufficient input validation of some parameters passed to the web-based management interface. An attacker could exploit this vulnerability by convincing a user of the interface to click a specific link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the interface or allow the attacker to access sensitive browser-based information. For information about fixed software releases, consult the Cisco bug ID at https://quickview.cloudapps.cisco.com/quickview/bug/CSCvn64652. When considering software upgrades, customers are advised to regularly consult the advisories for Cisco products, which are available from the Cisco Security Advisories and Alerts page, to determine exposure and a complete upgrade solution. |
| [CVE-2018-9920](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-9920) | Server side request forgery exists in the runtime application in K2 smartforms 4.6.11 via a modified hostname in an https://\*/Identity/STS/Forms/Scripts URL.  |
| [CVE-2018-8025](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-8025) | CVE-2018-8025 describes an issue in Apache HBase that affects the optional "Thrift 1" API server when running over HTTP. There is a race-condition which could lead to authenticated sessions being incorrectly applied to users, e.g. one authenticated user would be considered a different user or an unauthenticated user would be treated as an authenticated user. https://issues.apache.org/jira/browse/HBASE-20664 implements a fix for this issue. It has been fixed in versions: 1.2.6.1, 1.3.2.1, 1.4.5, 2.0.1 |

1. **Rf-moonlight.com**

|  |  |
| --- | --- |
| [CVE-2019-7675](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7675) | An issue was discovered on MOBOTIX S14 MX-V4.2.1.61 devices. The default management application is delivered over cleartext HTTP with Basic Authentication, as demonstrated by the /admin/index.html URI.  |
| [CVE-2019-7323](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7323) | GUP (generic update process) in LightySoft LogMX before 7.4.0 does not properly verify the authenticity of updates, which allows man-in-the-middle attackers to execute arbitrary code via a Trojan horse update. The update process relies on cleartext HTTP. The attacker could replace the LogMXUpdater.class file.  |
| [CVE-2019-6802](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-6802) | CRLF Injection in pypiserver 1.2.5 and below allows attackers to set arbitrary HTTP headers and possibly conduct XSS attacks via a %0d%0a in a URI.  |
| [CVE-2019-6500](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-6500) | In Axway File Transfer Direct 2.7.1, an unauthenticated Directory Traversal vulnerability can be exploited by issuing a specially crafted HTTP GET request with %2e instead of '.' characters, as demonstrated by an initial /h2hdocumentation//%2e%2e/ substring.  |
| [CVE-2019-6447](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-6447) | The ES File Explorer File Manager application through 4.1.9.7.4 for Android allows remote attackers to read arbitrary files or execute applications via TCP port 59777 requests on the local Wi-Fi network. This TCP port remains open after the ES application has been launched once, and responds to unauthenticated application/json data over HTTP.  |
| [CVE-2019-6256](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-6256) | A Denial of Service issue was discovered in the LIVE555 Streaming Media libraries as used in Live555 Media Server 0.93. It can cause an RTSPServer crash in handleHTTPCmd\_TunnelingPOST, when RTSP-over-HTTP tunneling is supported, via x-sessioncookie HTTP headers in a GET request and a POST request within the same TCP session. This occurs because of a call to an incorrect virtual function pointer in the readSocket function in GroupsockHelper.cpp.  |
| [CVE-2019-5489](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-5489) | The mincore() implementation in mm/mincore.c in the Linux kernel through 4.19.13 allowed local attackers to observe page cache access patterns of other processes on the same system, potentially allowing sniffing of secret information. (Fixing this affects the output of the fincore program.) Limited remote exploitation may be possible, as demonstrated by latency differences in accessing public files from an Apache HTTP Server.  |
| [CVE-2019-3822](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-3822) | libcurl versions from 7.36.0 to before 7.64.0 are vulnerable to a stack-based buffer overflow. The function creating an outgoing NTLM type-3 header (`lib/vauth/ntlm.c:Curl\_auth\_create\_ntlm\_type3\_message()`), generates the request HTTP header contents based on previously received data. The check that exists to prevent the local buffer from getting overflowed is implemented wrongly (using unsigned math) and as such it does not prevent the overflow from happening. This output data can grow larger than the local buffer if very large 'nt response' data is extracted from a previous NTLMv2 header provided by the malicious or broken HTTP server. Such a 'large value' needs to be around 1000 bytes or more. The actual payload data copied to the target buffer comes from the NTLMv2 type-2 response header. |