INCIDENT REPORT

Organization	Institute of Electrical and Electronics Engineers
Date	March 05,2018
Service	MSS-VME
Severity Level	Critical
Impact Level	Critical
Vulnerability Level	Critical

Our Operations Center (GOC), has detected the following vulnerabilities three vulnerabilities and recommends immediate remediation.

Affected Systems

http://208.99.166.235/index.php?action=Authenticate.login

Description

1. **According to its banner, the version of PHP 5.5.x running on the remote web server is prior to 5.5.24. It is, therefore, affected by multiple vulnerabilities:**

    - An out-of-bounds read error exists in the Phar component due to improper validation of user-supplied input when handling phar parsing during unserialize() function calls. An unauthenticated, remote attacker can exploit this to cause a denial of service condition or the disclosure of memory contents.

    - An unspecified use-after-free error exists in the _zend_shared_memdup() function within file ext/opcache/zend_shared_alloc.c that allows an unauthenticated, remote attacker to have an unspecified impact.

    - - A NULL pointer dereference flaw exists in the build_tablename() function within file pgsql.c in the PostgreSQL extension due to a failure to validate token extraction for table names. An authenticated,

remote attacker can exploit this, via a crafted name, to cause a denial of service condition.

Output

```
Version source    : X-Powered-By: PHP/5.5.16
Installed version : 5.5.16
Fixed version     : 5.5.24
```

Solution
Upgrade to PHP version 5.5.24 or later

2. Vulnerabilities related to protocols SSL / TLS (SSL Medium Strength Cipher Suites Supported)

- Those encryption suites that use DES, 3DES and IDEA algorithms and the SHA-1 hash algorithm are considered insecure.

Output
Here is the list of medium strength SSL ciphers supported by the remote server:

```
Here is the list of medium strength SSL ciphers supported by the remote server :

  Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

    EDH-RSA-DES-CBC3-SHA         Kx=DH          Au=RSA      Enc=3DES-CBC(168)        Mac=SHA1
    ECDHE-RSA-DES-CBC3-SHA       Kx=ECDH        Au=RSA      Enc=3DES-CBC(168)        Mac=SHA1
    DES-CBC3-SHA                 Kx=RSA         Au=RSA      Enc=3DES-CBC(168)        Mac=SHA1

The fields above are :

  {OpenSSL ciphername}
  Kx={key exchange}
  Au={authentication}
  Enc={symmetric encryption method}
  Mac={message authentication code}
  {export flag}
```

Solution
GLESEC, recommends eliminating all the entries related to the aforementioned algorithms from the suite.

3. SSL Certificate Cannot Be Trusted

Output

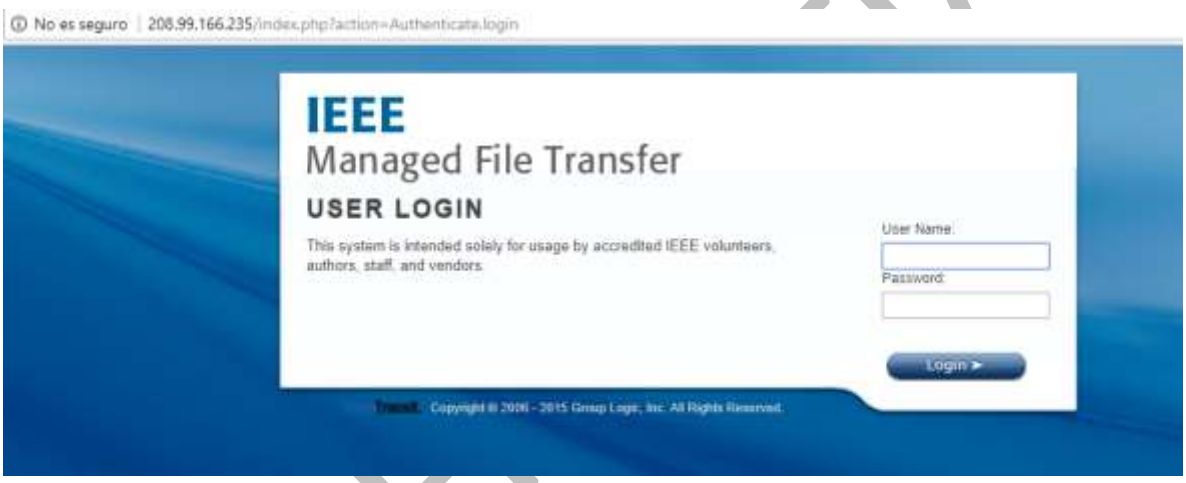
```
The following certificate was at the top of the certificate
chain sent by the remote host, but it is signed by an unknown
certificate authority :

|-Subject : C=US/ST=New Jersey/L=Piscatwaway/O=IEEE/OU=IT-Systems Analysts/CN=*.ieee.org
|-Issuer  : C=US/O=Entrust, Inc./OU=See www.entrust.net/legal-terms/OU=(c) 2012 Entrust, Inc. -
for authorized use only/CN=Entrust Certification Authority - L1K
```

Solution

Purchase or generate a proper certificate for this service.

We attach the image, showing the stated above.



GLESEC recommends applying these recommendations as soon as possible, in order to mitigate the risk of exploitation of these vulnerabilities.

For any questions please do not hesitate to contact us.

Sincerely,

GLESEC OPERATIONS CENTER – GOC.