GovCERT.HK

Weekly IT Security News Bulletin, 2017-W28

10 July – 16 July 2017

Headlines

Hundreds of domains hijacked

- Gandi is a French domain name registrar accredited by "Internet Corporation For Assigned Names and Numbers" (ICANN) and manages more than 2.1 million domain names across 730 top-level domains (TLDs). It reported that its name servers (NS) records of 751 domain names under 34 country-code or geographical TLDs were surreptitiously modified, causing access of the domains being redirected to malicious web servers for up to 11 hours on 7.7.2017.

- Those affected records used to be updated via a web portal of one of Gandi's technical partners. The breach was made by the attacker accessing the web portal using Gandi's login credentials, which were suspected to be leaked from insecure http only connections to the web portal.

- In addition to reversing the malicious changes, the registrar reset all login credentials for all of its technical platforms used to propagate Domain Name System (DNS) records. It has also launched a security audit on its whole infrastructure.

Advice

- Deploy HTTPS for websites to minimise risk of information leakage in transit, especially for login credentials.

- Apply extra security measures, such as multi-factor/multi-step authentication and IP restriction for updating DNS records.

- Enforce HTTP Strict Transport Security (HSTS) for HTTPS websites so that browsers which have visited the websites previously would be forced to use a valid HTTPS connection, not able to be emulated by redirected spoofing websites.

- Adopt DNSSEC as an extra layer of security against rogue records over the DNS infrastructure.

Sources

- Gandi Incident Report
- SCRT Blog
- Switch Security-Blog
- The Register

Defend your website with ZIP bombs

- Austrian security researcher, Christian Haschek, advises to put a "Zip bomb" on websites to stop hackers from scanning for vulnerabilities and gaining unauthorised access.

- The idea is to create a gigantic file filled with zeros and compress it into a much smaller ".gzip" file. A PHP script is used to deliver the file or the zip bomb to the vulnerability scanners or web browsers used by the hackers trying to visit protected web contents, such as program directories, admin panels, etc. The scanner or browser will start to decompress the big zip bomb, which holds up its resources. From Haschek's research, Nikto, SQLmap, IE 11, Chrome, Edge, Safari would be crashed as a result.

- The PHP script can also be tailored to check against the HTTP user agents of common vulnerability scanners and other conditions to block scanning of the whole website by these scanners and script kiddies who have no idea on how to change their user agent parameters. It is up to the imagination of web administrators to deploy the Zip bomb to defend their websites.

Advice

- Test the zip bomb in non-production environment to understand fully its impact on both hackers and legitimate users, before deploying it to production.

- Keep monitoring the web access logs to assess the effectiveness of the zip bomb deployment.

- Review regularly the deployment approach (such as where to put the zip bombs and what conditions to trigger) against changes in system environment as well as evolving hacking methods.

Sources

- Hascherk's Blog
- Bleeping Computer

Product Vulnerability Notes & Security Updates

1. **ABB VSN300 WiFi Logger Card**
   https://ics-cert.us-cert.gov/advisories/ICSA-17-192-03

2. **Adobe Flash Player**
   https://helpx.adobe.com/security/products/flash-player/apsb17-21.html
   https://www.hkcert.org/my_url/en/alert/17071202

3. **Apache HTTP Server**
   http://httpd.apache.org/security/vulnerabilities_22.html
   http://httpd.apache.org/security/vulnerabilities_24.html

4. **Apache Struts**
   https://struts.apache.org/docs/s2-048.html

5. **CentOS**
   https://lists.centos.org/pipermail/centos-announce/2017-July/022496.html
   https://lists.centos.org/pipermail/centos-announce/2017-July/022497.html

6. **Debian**
   https://www.debian.org/security/2017/dsa-3904
   https://www.debian.org/security/2017/dsa-3905
   https://www.debian.org/security/2017/dsa-3906
   https://www.debian.org/security/2017/dsa-3907
   https://www.debian.org/security/2017/dsa-3908

7. **F5 Products**
   https://support.f5.com/csp/article/K15412203
   https://support.f5.com/csp/article/K20486351
   https://support.f5.com/csp/article/K21154730
   https://support.f5.com/csp/article/K22317030
   https://support.f5.com/csp/article/K23030550
   https://support.f5.com/csp/article/K34125394
   https://support.f5.com/csp/article/K51931024
   https://support.f5.com/csp/article/K52114338
   https://support.f5.com/csp/article/K57211290
   https://support.f5.com/csp/article/K81601350
   https://support.f5.com/csp/article/K83043359

8. **FreeBSD**
   https://www.freebsd.org/security/advisories/FreeBSD-SA-17:05.heimdal.asc

9. **Fuji Electric V-Server**
   https://ics-cert.us-cert.gov/advisories/ICSA-17-192-02

10. **GE Communicator**
    https://ics-cert.us-cert.gov/advisories/ICSA-17-194-02

11. **Gentoo Linux**
    https://security.gentoo.org/glsa/201707-03
    https://security.gentoo.org/glsa/201707-04

https://security.gentoo.org/glsa/201707-05
https://security.gentoo.org/glsa/201707-06
https://security.gentoo.org/glsa/201707-07
https://security.gentoo.org/glsa/201707-08
https://security.gentoo.org/glsa/201707-09
https://security.gentoo.org/glsa/201707-10
https://security.gentoo.org/glsa/201707-11
https://security.gentoo.org/glsa/201707-12
https://security.gentoo.org/glsa/201707-13
https://security.gentoo.org/glsa/201707-14

12. **IBM InfoSphere Information Server**
    http://www-01.ibm.com/support/docview.wss?uid=swg22004602
    http://www-01.ibm.com/support/docview.wss?uid=swg22004729

13. **IBM WebSphere Application Server**
    http://www-01.ibm.com/support/docview.wss?uid=swg22003240

14. **Juniper Products**
    https://kb.juniper.net/InfoCenter/index?page=content&id=JSA10782
    https://kb.juniper.net/InfoCenter/index?page=content&id=JSA10791
    https://kb.juniper.net/InfoCenter/index?page=content&id=JSA10794
    https://kb.juniper.net/InfoCenter/index?page=content&id=JSA10797

15. **Mageia**
    http://advisories.mageia.org/MGASA-2017-0201.html
    http://advisories.mageia.org/MGASA-2017-0202.html
    http://advisories.mageia.org/MGASA-2017-0203.html
    http://advisories.mageia.org/MGASA-2017-0204.html
    http://advisories.mageia.org/MGASA-2017-0205.html
    http://advisories.mageia.org/MGASA-2017-0206.html
    http://advisories.mageia.org/MGASA-2017-0207.html

16. **Microsoft Products**
    https://portal.msrc.microsoft.com/en-us/security-guidance/releasenotedetail/f2b16606-4945-e711-80dc-000d3a32fc99
    https://support.microsoft.com/en-us/help/20170711/security-update-deployment-information-july-11-2017
    https://www.hkcert.org/my_url/en/alert/17071201

17. **openSUSE**
    https://lists.opensuse.org/opensuse-security-announce/2017-07/msg00010.html
    https://lists.opensuse.org/opensuse-security-announce/2017-07/msg00011.html
    https://lists.opensuse.org/opensuse-security-announce/2017-07/msg00016.html

18. **Oracle Linux**
    https://linux.oracle.com/errata/ELSA-2017-1721.html
    https://linux.oracle.com/errata/ELSA-2017-1723.html
    https://linux.oracle.com/errata/ELSA-2017-3592.html

19. **OSIsoft PI Products**
    https://ics-cert.us-cert.gov/advisories/ICSA-17-192-04
    https://ics-cert.us-cert.gov/advisories/ICSA-17-192-05

20. **PHP**
    http://php.net/ChangeLog-5.php#5.6.31
    http://php.net/ChangeLog-7.php#7.0.21
    http://php.net/ChangeLog-7.php#7.1.7

21. **Red Hat**
    https://access.redhat.com/errata/RHSA-2017:1715
    https://access.redhat.com/errata/RHSA-2017:1721
    https://access.redhat.com/errata/RHSA-2017:1723
    https://access.redhat.com/errata/RHSA-2017:1731
    https://access.redhat.com/errata/RHSA-2017:1739

22. **Samba**
    https://www.samba.org/samba/security/CVE-2017-11103.html
    https://www.hkcert.org/my_url/en/alert/17071301

23. **Schweitzer Engineering Laboratories, Inc. Ethernet Security Gateway**
    https://ics-cert.us-cert.gov/advisories/ICSA-17-192-06

24. **Siemens Products**
    https://ics-cert.us-cert.gov/advisories/ICSA-17-194-01
    https://ics-cert.us-cert.gov/advisories/ICSA-17-194-03

25. **Slackware**
    http://www.slackware.com/security/viewer.php?l=slackware-security&y=2017&m=slackware-security.344641
    http://www.slackware.com/security/viewer.php?l=slackware-security&y=2017&m=slackware-security.347794
    http://www.slackware.com/security/viewer.php?l=slackware-security&y=2017&m=slackware-security.436661
    http://www.slackware.com/security/viewer.php?l=slackware-security&y=2017&m=slackware-security.438658
    http://www.slackware.com/security/viewer.php?l=slackware-security&y=2017&m=slackware-security.560479

26. **SUSE**
    https://www.suse.com/support/update/announcement/2017/suse-su-20171812-1.html
    https://www.suse.com/support/update/announcement/2017/suse-su-20171813-1.html
    https://www.suse.com/support/update/announcement/2017/suse-su-20171815-1.html
    https://www.suse.com/support/update/announcement/2017/suse-su-20171821-1.html
    https://www.suse.com/support/update/announcement/2017/suse-su-20171832-1.html
    https://www.suse.com/support/update/announcement/2017/suse-su-20171835-1.html
    https://www.suse.com/support/update/announcement/2017/suse-su-20171836-1.html
    https://www.suse.com/support/update/announcement/2017/suse-su-20171837-1.html
    https://www.suse.com/support/update/announcement/2017/suse-su-20171838-1.html
    https://www.suse.com/support/update/announcement/2017/suse-su-20171839-1.html
    https://www.suse.com/support/update/announcement/2017/suse-su-20171848-1.html
    https://www.suse.com/support/update/announcement/2017/suse-su-20171850-1.html
    https://www.suse.com/support/update/announcement/2017/suse-su-20171853-1.html

27. **Trend Micro Control Manager 6.0**
    https://success.trendmicro.com/solution/1117722

28. **Ubuntu**

https://www.ubuntu.com/usn/usn-3350-1/
https://www.ubuntu.com/usn/usn-3351-1/
https://www.ubuntu.com/usn/usn-3352-1/

Sources of product vulnerability information:

Adobe
Apache Struts
Apache HTTPD
CentOS
Debian
F5
FreeBSD
Gentoo Linux
HKCERT
IBM
ICS-CERT
Juniper
Mageia
Microsoft
openSUSE
Oracle Linux
PHP
Red Hat
Samba
Trend Micro
Slackware
SUSE
Ubuntu

Contacts:

cert@govcert.gov.hk