Start Commercial (StartCom) Limited

StartSSL™ Certificates & Public Key Infrastructure

Eilat, Israel

Critical Event Report

Date: **Saturday December 20th 2008**

Start: **0:00**

End: **7:30**

Summary:

From the night of Friday to Saturday at the 20th of December a new subscriber named “Mike Zusman” registered at the CA site with gmail account mikezusman@gmail.com. Subsequently he succeeded in overcoming the domain validation interface by validating for domains not under his control with this email address. At the attempt to create a certificate for verisign.com, a high profile target was detected by the underlying system and the certificate was flagged for review. Minutes later the attempt was analyzed and detected as fraudulent, the subscriber blocked from accessing the system and all server certificates were revoked immediately. During an email exchange with Mike in which he cooperated, he disclosed the attack vector, the attack was reproduced. Consequently steps were taken to prevent such occurrence and the system was modified accordingly. Modification was tested and approved. Evidence of the attack is stored, criminal charges are not pursued at the writing of this report.

Time line:

- 2008-12-19 23:24 – Registration by the attacker “Mike Zusman”.
- 2008-12-19 23:32 – First attempt for fraudulent domain validation using domain dishuplink.com which failed.
- 2008-12-19 23:37 – Second attempt for fraudulent domain validation using domain phishme.com and email address mikezusman@gmail.com succeeded.
- 2008-12-19 23:44 – Server certificate for phishme.com was issued.
- 2008-12-19 23:57 – Third attempt for domain validation using domain intrepidusgroup.com succeeded.
- 2008-12-20 00:03 – Server certificate for intrepidusgroup.com was issued.
- 2008-12-20 00:33 – Forth attempt for domain validation using domain paypal.com succeeded.
- 2008-12-20 00:54 – Fifth attempt for domain validation using domain verisign.com succeeded.

Start Commercial (StartCom) Limited

StartSSL™ Certificates & Public Key Infrastructure

Eilat, Israel

- 2008-12-20 01:09 – Server certificate for verisign.com was flagged and not issued – attempt failed.
- 2008-12-20 01:17 – Attack was detected and the attacker contacted. IP address 68.197.203.233 was blocked at the firewall.
- 2008-12-20 01:19 - All server certificates produced by the attacker are revoked and a new CRL issued (automatically).
- 2008-12-20 01:23 – Attacker replied to the first email and vowed cooperation.
- 2008-12-20 02:00 – The attack was fully disclosed which involved proxying ,intercepting all communication from and to the browser and eventually modification of the browser response to the server. A tool like http://www.owasp.org/index.php/Category:OWASP_WebScarab_Project was used for the attack.
- 2008-12-20 03:20 – First modification and testing done on the system to prevent this type of attacks.
- 2008-12-20 03:25 – Emergency fix confirmed to prevent occurrence of this attack.
- 2008-12-20 07:30 – Modifications confirmed to be effective and thwart this type of attacks.
- 2008-12-20 15:06 – Other elements which might have been also subject to this type of attacks were analyzed, modifications applied, tested and approved.
- 2008-12-20 16:00 – Writing this report closes this event.

Steps taken:

Upon detection, the attacker was contacted, IP address 68.197.203.233 banned from the StartCom network and all server certificates of the attacker revoked within a few minutes. The attack was analyzed, and preventive measures taken. The upper management of StartCom was informed since the first minutes and throughout the event, including resolution. The system was modified to avert this kind of attacks initially in an emergency bug fix, during the subsequent hours other possible points of failure possibly subject to the same attack vector analyzed and the initial modifications improved, tested for failure and success using the same tools used by the attacker. The attacker proved to be cooperative, evidence was recorded and criminal charges currently not taken.

Final conclusion:

The use of a high profile target by the attacker enabled detection of the attack by the system and within minutes personnel acted with preventive steps. Disclosure

of the attack helped understand the attack vector and allowed to reproduce the attack quickly. Subsequent modifications removed this vulnerability completely. The attack was contained within one hour and the system modified within three hours of the first attack. Subsequent improvements, testing, reproduction of the attack were performed and the event closed within fourteen hours of the attack. No damage was done to any relying party, certificates were revoked within less than one hour, which made it impossible to have any impact for fraudulent use. No high-profile target certificate was issued during this event. Only low-assurance Class 1 certificates were involved.

Approvals:

Eddy Nigg, COO/CTO

Revital Nigg, CEO