DECISION GROUP

Security Concerns in E-Detective System

Response to the Enquiry of International Business Times, UK

Few days ago, we got the enquiry of system security concerns in E-Detective from International Business Times[1]. The enquiry is at the vulnerability point of unauthenticated user to read arbitrary files on the system. This may include database credentials and captured data intercepts.

Actually we are fully aware of such security concern since 4 years ago when our client asked to enhance the security level of E-Detective system. The most important guideline of E-Detective deployment is that E-Detective should be deployed in the closed network domain without Internet access to outside world. This network domain should be also isolated from other corporate or government service network segment. By this way, only few authentic staff can access the internal system.

Since all users of E-Detective are of 4 types: operator, administrator, auditor and datamvr. Operator has the authorized right to input queries and view the scope of intercepted data by his/her own right. Administrator can have authorized right to conduct the operation of system backup, user management, and software system tuning…etc. Auditor has the only right to check and view all log files in the system. The last type of user is only for data transport between different systems, and it cannot be used for system access. None of these users has the superuser right of root. In most cases, root is basically set to hibernation status after system is activated by license under customer SLA request in order to terminate security backdoor.

Besides, E-Detective can be integrated with OTP server for more secured access control, and all logon access record will be reviewed in OTP server for auditing. Biometric access mechanism module with fingerprint can be also available by customer request, but it depends on whether the fingerprint reader is supported on user workstation.

After all, E-Detective system is used by our customer for network forensic purpose, such as internal data leakage protection, cyber evidence collection and lawful interception. System security is always the top priority for our customer. All the vulnerabilities mentioned in the news by International Business Times have been fixed several months ago. “Customer IT security is always our top concern,” said Casper Kan Chang, CEO of Decision Group, “and we have already fixed all the vulnerabilities in this current version of E-Detective for more than 11 months.” For those existing customers with old version of system still has concern, Decision Group will update it for free without hesitation.

If you have any request or question about the security mechanism, please contact with us by: service@decision.com.tw. We will be happy to fulfill your request.

[1] http://www.ibtimes.co.uk/e-detective-spying-tool-used-by-over-100-law-enforcement-agencies-has-major-security-holes-1506447

Address : 4/F NO. 31, ALLEY 4, LANE 36, SEC 5, MING-SHEN EAST ROAD,TAIPEI 105, TAIWAN, R.O.C.
TEL : +886-2-27665753 / 27695496 FAX : +886-2-27665702 / 27569591 URL : www.decision.com.tw