25 Ιουνίου 2015

NetNanny: Προβλήματα στο certification – κινδυνεύουν οι χρήστες

/ Πεμπτουσία

Image not found or type unknown

Το NETNANNY, το δημοφιλές software ελέγχου περιεχομένου, βρέθηκε να χρησιμοποιεί ένα shared private key και ένα root certificate authority που το αφήνει εκτεθειμένο σε HTTPS spoofing και επίθεση.

«Το certificate που χρησιμοποιείται από το NETNANNY βρίσκεται σε όλες τις εγκαταστάσεις του NETNANNY,» ανέφερε ο Garret Wassermann, ένας αναλυτής ευπαθειών της εταιρείας CERT. Πρόσθεσε ότι «το private key που χρησιμοποιείται για να παραγάγει το πιστοποιητικό, μοιράζεται, και μπορεί επίσης να ληφθεί ως plain text κατευθείαν από το λογισμικό.»

Ένας επιτιθέμενος μπορεί εύκολα να εκμεταλλευτεί αυτόν τον περιορισμό για να παραγάγει τα νέα πιστοποιητικά με την πρόσβαση του στο λογισμικό. Το spoofed certificate που υπογράφεται από το NETNANNY θα εμφανιζόταν ως αξιόπιστο και θα οδηγούσε το χρήστη σε ένα κακόβουλο site, το οποίο θα εμφανιζόταν ως ψευδές secure HTTPS site.

Το software NETNANNY, που δημιουργήθηκε από το 1995, χρησιμοποιείται ευρέως από τους γονείς για να φιλτράρουν τις υπηρεσίες του Διαδικτύου για τα παιδιά

τους. Προς το παρόν στην έκδοση 7.2.4.2 έχει βρεθεί με ευπάθεια, σύμφωνα με την προειδοποίηση του CERT. Οι ερωτήσεις σχετικά με την αποκατάσταση του προβλήματος παραμένουν αναπάντητες από την ContentWatch, την εταιρεία developing.

Οι χρήστες συμβουλεύονται να αφαιρέσουν το NETNANNY ή τουλάχιστον να αφαιρέσουν τα ψευδή πιστοποιητικά που δημιουργούνται από την υπηρεσία, ή να θέσουν εκτός λειτουργίας το SSL filtering και να αφαιρέσουν χειροκίνητα τα πιστοποιητικά από εκεί.

Πηγή: SecNews.gr