Διασφάλιση των βασικών αρχών για την ανάπτυξη λογισμικού

Με τη δραματική αύξηση των κρατικών επιθέσεων στον κυβερνοχώρο και των κακόβουλων φορέων στο διαδίκτυο, πιστεύουμε ότι οι υπηρεσίες και τα προϊόντα μας είναι χρήσιμα στον βαθμό που είναι ασφαλή. Στην Google, εστιάζουμε περισσότερο από ποτέ στην προστασία των ανθρώπων, των οργανισμών και των κυβερνήσεων, με το να μοιραζόμαστε την τεχνογνωσία μας, να ενισχύουμε την κοινωνία για την αντιμετώπιση των διαρκώς εξελισσόμενων κινδύνων στον κυβερνοχώρο και με το να εργαζόμαστε συνεχώς για την εξέλιξη της τεχνολογίας στον τομέα της κυβερνοασφάλειας, ώστε να δημιουργήσουμε έναν ασφαλέστερο κόσμο για όλους.

Το λογισμικό ανοικτού κώδικα — δηλαδή ο κώδικας που διατίθεται ελεύθερα σε οποιονδήποτε για χρήση, τροποποίηση και αξιοποίηση — είναι το θεμέλιο του σύγχρονου διαδικτύου. Ο χώρος της ανάπτυξης λογισμικού ανοικτού κώδικα επιτρέπει τη συνεργασία και την ταχύτατη καινοτομία μέσω της ελεύθερης ανταλλαγής λύσεων. Ωστόσο, η ίδια η διαφάνεια που καθιστά τον ψηφιακό κόσμο προσβάσιμο σε όλους, τον κάνει επίσης μοναδικά ευάλωτο σε απειλές ασφάλειας.

Πρόκληση

Το λογισμικό ανοικτού κώδικα προβληματίζει τους πάντες

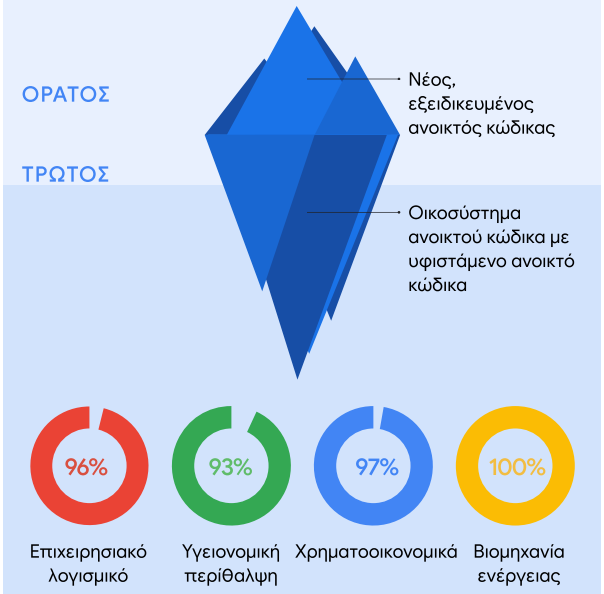
Η κοινότητα ανάπτυξης ανοικτού κώδικα, η οποία βασίζεται στη διαφάνεια και την κοινή χρήση, συμβάλλει με τεράστιο όγκο κώδικα στην πλειονότητα των εφαρμογών που χρησιμοποιούμε σήμερα. Από τον ιατρικό εξοπλισμό έως το ηλεκτρικό δίκτυο, οι άνθρωποι βασίζονται στο λογισμικό ανοικτού κώδικα (OSS) σχεδόν κάθε ώρα της ημέρας, γεγονός που καθιστά τα έργα ανοικτού κώδικα πρωταρχικό στόχο για επιθέσεις στον κυβερνοχώρο. Τα τελευταία τρία χρόνια σημειώθηκε αύξηση κατά 742% σε ετήσια βάση[1] στις επιθέσεις στην αλυσίδα εφοδιασμού λογισμικού.

Το οικοσύστημα ανοικτού κώδικα είναι πολύπλοκο και πολυεπίπεδο, με κρυφές έμμεσες εξαρτήσεις που μπορεί να εμπεριέχουν κενά ασφάλειας. Αυτά τα επίπεδα καθιστούν δύσκολη την ανίχνευση των τρωτών σημείων με μη αυτόματο τρόπο και η διασφάλιση αυτού του τμήματος της ανάπτυξης λογισμικού έχει καταστεί επείγον ζήτημα ασφάλειας σε παγκόσμιο επίπεδο.

Απαιτείται μεγαλύτερη έμφαση σε όλα τα επίπεδα

- Οι προγραμματιστές ανοικτού κώδικα χρειάζονται γνώσεις και πόρους για να προστατεύσουν τα έργα τους.
- Οι οργανισμοί πρέπει να κατανοήσουν τους κινδύνους και τα τρωτά σημεία της αλυσίδας εφοδιασμού για να αναπτύξουν σχέδια μετριασμού.
- Οι κυβερνήσεις και ο κλάδος οφείλουν να συνεργαστούν για να εξασφαλίσουν ισχυρά και αποτελεσματικά πρότυπα ασφάλειας.[3]

ΤΟ ΠΟΣΟΣΤΟ ΤΟΥ ΛΟΓΙΣΜΙΚΟΥ ΤΟΥ ΚΛΑΔΟΥ ΠΟΥ ΠΕΡΙΛΑΜΒΑΝΕΙ ΑΝΟΙΚΤΟ ΚΩΔΙΚΑ[2]



[2] Πηγή: 2022 Synopsys Open Source Security and Risk Analysis Report

Η λύση μας

Διασφάλιση του λογισμικού ανοικτού κώδικα για όλους

Στην Google εργαζόμαστε εδώ και χρόνια πάνω σε αυτήν την πρόκληση. Στην πραγματικότητα, κάθε χρόνο πάνω από το 10% των εργαζομένων της Google συνεισφέρουν σε έργα λογισμικού ανοικτού κώδικα. Η εμπειρία μας μάς οδηγεί στο συμπέρασμα ότι μπορεί να επιτευχθεί σύγχρονη ψηφιακή ασφάλεια, εάν υιοθετήσουμε τη διαφάνεια. Οι ανοικτές προσεγγίσεις διασφαλίζουν ότι μπορούμε να υιοθετήσουμε γρήγορα τις τελευταίες καινοτομίες και να επιτρέψουμε σε περισσότερους ανθρώπους να επιλύσουν προκλήσεις στον τομέα της ασφάλειας. Ωστόσο, για να «ξεκλειδώσουμε» πλήρως την αξία του ανοικτού κώδικα χρειαζόμαστε ισχυρότερες συνεργασίες μεταξύ δημόσιου και ιδιωτικού τομέα και ένα δυναμικό πλαίσιο πολιτικής για την ενίσχυση της ασφάλειας για όλους. Αυτός είναι ο λόγος για τον οποίο επικροτούμε τις προσπάθειες της αμερικανικής κυβέρνησης για την προώθηση της ασφάλειας του λογισμικού ανοικτού κώδικα (OSS), όπως ο Νόμος για την Προστασία του Λογισμικού Ανοικτού Κώδικα που κατατέθηκε στη Γερουσία το 2022.

- Καθοδηγούμε την κοινότητα με πλαίσια ασφάλειας επόμενου επιπέδου, όπως το Supply-chain Levels for Software Artifacts (SLSA),[4,5] και αναπτύσσουμε προηγμένα εργαλεία ασφάλειας.
- Αναπτύξαμε το γράφημα GUAC (Graph for Understanding Artifact Composition), το οποίο συγκεντρώνει πληροφορίες για την ασφάλεια λογισμικού από διαφορετικές πηγές σε μια ενιαία βάση δεδομένων με δυνατότητα αναζήτησης. Το GUAC θα εκδημοκρατίσει τη διαθεσιμότητα των πληροφοριών ασφάλειας, καθιστώντας τες ελεύθερα προσβάσιμες και χρήσιμες για κάθε οργανισμό.

Οι δεσμεύσεις μας:

- Επένδυση 100 εκατομμυρίων δολαρίων στην ασφάλεια ανοικτού κώδικα, ηγετικοί ρόλοι στο Ίδρυμα Ασφάλειας Ανοικτού Κώδικα και άμεση συνεργασία με τους προγραμματιστές.
- Καθορισμός και διαμοιρασμός εφαρμόσιμων προτύπων ασφάλειας, καθοδήγησης, δωρεάν εργαλείων και βέλτιστων πρακτικών που χρησιμοποιούμε εσωτερικά, με όλη την κοινότητα ανοικτού κώδικα.
- Προώθηση της ανίχνευσης, αυτοματοποιημένη ταξινόμηση και τρόποι ενσωμάτωσης της ασφάλειας στα πρώτα στάδια ανάπτυξης.
- Αυτοματοποίηση εργαλείων για να καταστήσουμε την επιχειρησιακή ασφάλεια δωρεάν και προσιτή σε όλους.

Εφαρμογές

Το έργο OSS-Fuzz από την Google
Η απάντησή μας στο σφάλμα Heartbleed

Το σφάλμα Heartbleed ήταν ένα σοβαρό τρωτό σημείο ανοικτού κώδικα, μια αδυναμία που είχε τη δυνατότητα να επηρεάσει σχεδόν κάθε χρήστη στο διαδίκτυο. Το 2014, χάκερ έκλεψαν τα ονόματα, τις διευθύνσεις, τις ημερομηνίες γέννησης, τους αριθμούς τηλεφώνου και τους αριθμούς κοινωνικής ασφάλισης περίπου 4,5 εκατομμυρίων ασθενών από τη βάση δεδομένων ενός από τα μεγαλύτερα νοσοκομεία των ΗΠΑ.

Ως απάντηση, η Google εγκαινίασε το έργο OSS-Fuzz ως δωρεάν υπηρεσία για την κοινότητα. Οι δοκιμές Fuzz εντοπίζουν άγνωστες αδυναμίες ασφάλειας μέσα σε λίγα λεπτά, σε αντίθεση με τον χειροκίνητο δοκιμαστικό έλεγχο, ο οποίος μπορεί να διαρκέσει μήνες. Επενδύσαμε στη δημιουργία μιας υποδομής για την αυτόματη δοκιμή εκατοντάδων έργων ανοικτού κώδικα. Το έργο OSS-Fuzz σαρώνει πλέον τακτικά τον κώδικα και καινοτομεί διαρκώς για να βρίσκει περισσότερες κατηγορίες σφαλμάτων.

800+ κρίσιμα έργα ανοικτού κώδικα σαρώνονται με δοκιμές Fuzz σε έξι γλώσσες.

Οι επενδύσεις μας στον κλάδο και τα ορόσημα

2020 — ΑΥΓΟΥΣΤΟΣ
Ενταχθήκαμε στο Ίδρυμα Ασφάλειας Ανοικτού Κώδικα (OpenSSF) για την καθοδήγηση και τη βελτίωση της ασφάλειας του λογισμικού ανοικτού κώδικα.

2021 — ΜΑΪΟΣ και ΙΟΥΝΙΟΣ
Καθιερώσαμε βέλτιστες πρακτικές OSS σύμφωνα με την εκτελεστική εντολή 14028 του Λευκού Οίκου και συνεισφέραμε στην καθοδήγηση σχετικά με τα πρότυπα ασφάλειας της αλυσίδας εφοδιασμού λογισμικού.

ΙΟΥΝΙΟΣ
Κυκλοφορήσαμε το πλαίσιο SLSA με το Ίδρυμα Ασφάλειας Ανοικτού Κώδικα (OpenSSF), εξωτερικεύοντας το εσωτερικό πλαίσιο ασφάλειας της Google και επιτρέποντας σε όλους να δημιουργούν ασφαλέστερο λογισμικό.

ΑΥΓΟΥΣΤΟΣ
Υποσχεθήκαμε 100 εκατομμύρια δολάρια για την αναβάθμιση και την ασφάλεια του OSS, συμπεριλαμβανομένης της συνεργασίας με προγραμματιστές για τον εντοπισμό και τη διόρθωση τρωτών σημείων.

2022 — ΜΑΪΟΣ
Ανακοινώσαμε το Συνεργείο Συντήρησης Ανοικτού Κώδικα της Google κατά τη διάρκεια **μιας συνόδου κορυφής στην Ουάσιγκτον,** αφιερώνοντας μια ομάδα προγραμματιστών πλήρους απασχόλησης που θα δουλεύουν αποκλειστικά σε έργα ανοικτού κώδικα για τη βελτίωση της ασφάλειάς τους.

ΜΑΪΟΣ
Ανακοινώσαμε το προϊόν Assured Open Source Software, το οποίο βοηθά στην ενσωμάτωση των ίδιων αξιόπιστων πακέτων ανοικτού κώδικα που χρησιμοποιεί η Google στις ροές εργασίας των προγραμματιστών.

Οι συνιστώμενες πρακτικές της Google που μπορούν να βοηθήσουν τους δημόσιους και ιδιωτικούς οργανισμούς να παραμείνουν ασφαλείς σήμερα:

- Εφαρμογή του πλαισίου SLSA για την ενίσχυση της ασφάλειας της αλυσίδας εφοδιασμού λογισμικού
- Κρυπτογραφική υπογραφή και επαλήθευση της αυθεντικότητας του λογισμικού σας με τη χρήση του Sigstore
- Αυτοματοποίηση της ανακάλυψης, παρακολούθησης και ταξινόμησης τρωτών σημείων με το OSS-Fuzz και το OSV.dev
- Χρήση καρτών βαθμολογίας για την αυτόματη αξιολόγηση του κινδύνου ασφάλειας με τις εξαρτήσεις σας

Η προσέγγισή μας

Το λογισμικό είναι τόσο ασφαλές όσο ο πιο αδύναμος κρίκος. Διαθέτουμε την τεχνογνωσία και τους οικονομικούς μας πόρους για να βελτιώσουμε την ασφάλεια ολόκληρου του οικοσυστήματος ανοικτού κώδικα. Η ομάδα των ειδικών μας σε θέματα ανάπτυξης και ασφάλειας πιστεύει ότι μπορούμε να προστατεύσουμε περισσότερους δημόσιους και ιδιωτικούς οργανισμούς με τους ακόλουθους τρόπους:

Η ομάδα μας επιθεωρεί διαρκώς κάθε στάδιο του κύκλου ζωής του προϊόντος, σαρώνοντας, αναλύοντας και ελέγχοντας με δοκιμές Fuzz για τρωτά σημεία.

Υποστηρίζουμε το ανοιχτό διαδίκτυο, κοινοποιώντας όσα γνωρίζουμε στην κοινότητα των προγραμματιστών και διατηρώντας το ασφαλές για το κοινό και τις επιχειρήσεις.

Φροντίζουμε για τη μελλοντική ασφάλεια με τον εντοπισμό εξελιγμένων απειλών, την παροχή προηγμένων αυτοματοποιημένων εργαλείων και παραμένοντας ένα βήμα μπροστά.

Η διασφάλιση του λογισμικού ανοικτού κώδικα είναι κοινή ευθύνη και δεσμευόμαστε για συνεχή συνεργασία σε αυτό το επείγον, κρίσιμο πρόβλημα. g.co/security/gosst

Πηγές: 1. 2022 State of the Software Supply Chain. 2. 2022 Synopsys Open Source Security and Risk Analysis Report. 3. CISA Goes on Tour to Get Feedback on Cyber Incident Reporting Rules. 4. Η κοινοποίηση των γνώσεών μας (π.χ., δημοσιεύοντας το πλαίσιο SLSA, καθοδηγώντας το ίδρυμα OpenSSF) συνεπάγεται ότι όλοι όσοι κατασκευάζουν λογισμικό, όχι μόνο η Google, μπορούν να επωφεληθούν από την εμπειρία και τις δοκιμασμένες πρακτικές ασφάλειας της Google. 5. Το πλαίσιο SLSA είναι ένα σύνολο πρακτικών οι οποίες μπορούν να βοηθήσουν τους οργανισμούς να βελτιώσουν την ασφάλεια της διαδικασίας ανάπτυξης λογισμικού τους. Βοηθά στην εκπλήρωση του Πλαισίου Ασφαλούς Ανάπτυξης Λογισμικού της κυβέρνησης των ΗΠΑ, απαιτήσεις που καθορίστηκαν από την κυβέρνηση ως απάντηση στο εκτελεστικό διάταγμα για την ασφάλεια στον κυβερνοχώρο. Αυτό σημαίνει ότι οι οργανισμοί θα έχουν καθοδήγηση σχετικά με τον τρόπο συμμόρφωσης με τις ομοσπονδιακές κατευθυντήριες γραμμές για να καταστήσουν το λογισμικό ασφαλέστερο για όλους.