Adrodd bregusrwydd

Mae'r polisi datgelu bregusrwydd hwn yn berthnasol i unrhyw bregusrwydd rydych chi'n ystyried eu hadrodd i ni (y "Sefydliad").

Rydym yn argymell darllen y polisi datgelu bregusrwydd hwn yn llawn cyn i chi adrodd am bregusrwydd ac eich bod bob amser yn gweithredu yn unol ag ef. Rydym yn gwerthfawrogi'r rhai sy'n cymryd yr amser a'r ymdrech i adrodd am bregusrwydd diogelwch yn unol â'r polisi hwn. Fodd bynnag, ni roddwn wobrau ariannol am ddatgelu bregusrwydd.

Cyflwyno Adroddiadau

Os ydych chi'n credu eich bod wedi dod o hyd i fregusrwydd diogelwch, cyflwynwch eich adroddiad atom drwy'r platfform HackerOne

Yn eich adroddiad, rhowch wybodaeth am:

Y wefan, IP neu dudalen lle gellir arsylwi'r bregusrwydd. Disgrifiad byr o'r math o fregusrwydd, er enghraifft; "XSS vulnerability". Camau i atgynhyrchu. Dylai'r rhain fod yn brawf cysyniad hynaws, annistrywiol. Mae hyn yn helpu i sicrhau y gellir frysbennu'r adroddiad yn gyflym ac yn gywir. Mae hefyd yn lleihau'r tebygolrwydd o adroddiadau dyblyg, neu ecsbloetio maleisus o rai gwendidau, fel meddiannu is-barth.

Beth i'w ddisgwyl

Ar ôl i chi gyflwyno'ch adroddiad, byddwn yn ymateb i'ch adroddiad o fewn pum diwrnod gwaith ac yn anelu at frysbennu eich adroddiad o fewn 10 diwrnod gwaith. Byddwn hefyd yn anelu at eich hysbysu o'n cynnydd.

Asesir blaenoriaeth ar gyfer adferiad trwy edrych ar yr effaith, difrifoldeb a chymhlethdod ecsbloetio. Gallai adroddiadau bregusrwydd gymryd peth amser i frysbennu neu fynd i'r afael â nhw. Mae croeso i chi holi am y statws ond dylech osgoi gwneud hynny fwy nag unwaith bob 14 diwrnod. Mae hyn yn caniatáu i'n timau ganolbwyntio ar yr adferiad.

Byddwn yn eich hysbysu pan fydd y bregusrwydd a adroddwyd yn cael ei adfer, ac efallai y cewch eich gwahodd i gadarnhau bod yr ateb yn cwmpasu'r bregusrwydd yn ddigonol.

Unwaith y bydd eich bregusrwydd wedi'i ddatrys, rydym yn croesawu ceisiadau i ddatgelu eich adroddiad. Hoffem uno canllawiau i ddefnyddwyr yr effeithir arnynt, felly parhewch i gydlynu datganiad cyhoeddus gyda ni.

Arweiniad

Rhaid i chi BEIDIO â:

- Torri unrhyw gyfraith neu reoliadau perthnasol.
- Cyrchu symiau diangen, gormodol neu sylweddol o ddata.
- Addasu data yn systemau neu wasanaethau'r Sefydliad.
- Defnyddio offer sganio ymledol neu ddinistriol dwysedd uchel i ddod o hyd i bregisrwydd.
- Ceisio neu adrodd unrhyw fath o wrthod gwasanaeth, e.e. gorlethu gwasanaeth gyda chyfaint uchel o geisiadau.
- Tarfu ar wasanaethau neu systemau'r Sefydliad.
- Cyflwyno adroddiadau sy'n manylu ar bregusrwydd na ellir eu hecsbloetio, neu adroddiadau sy'n dangos nad yw'r gwasanaethau yn cyd-fynd yn llawn â "arfer gorau", er enghraifft penawdau diogelwch ar goll. Cyflwyno adroddiadau sy'n manylu ar wendidau cyfluniad TLS, er enghraifft cefnogaeth cyfres seiffr "gwan" neu bresenoldeb cefnogaeth TLS1.0.
- Cyfathrebu unrhyw wendidau neu fanylion cysylltiedig heblaw trwy ddulliau a ddisgrifir yn y testun diogelwch cyhoeddedig.
- Peiriannu cymdeithasol, 'phishing' neu ymosod yn gorfforol ar staff neu seilwaith y Sefydliad.
- Gofyn am iawndal ariannol er mwyn datgelu unrhyw bregusrwydd.

Rhaid i chi:

- Cydymffurfio â rheolau diogelu data bob amser a pheidio â thorri preifatrwydd defnyddwyr, staff, contractwyr, gwasanaethau neu systemau'r Sefydliad. Rhaid i chi beidio, er enghraifft, rhannu, ailddosbarthu na methu â diogelu'n briodol data a adalwyd o'r systemau neu'r gwasanaethau.
- Dileu'r holl ddata a adalwyd yn ystod eich ymchwil yn ddiogel cyn gynted ag nad oes ei angen mwyach neu o fewn 1 mis i'r bregusrwydd gael ei ddatrys, pa un bynnag sy'n digwydd gyntaf (neu fel sy'n ofynnol fel arall gan gyfraith diogelu data).

Cyfreithlondeb

Mae'r polisi hwn wedi'i gynllunio i fod yn gydnaws ag arfer da datgelu bregusrwydd cyffredin. Nid yw'n rhoi caniatâd i chi weithredu mewn unrhyw ffordd sy'n anghyson â'r gyfraith, neu a allai achosi i'r Sefydliad neu sefydliadau partner fod yn torri unrhyw rwymedigaethau cyfreithiol.

Fodd bynnag, os yw camau cyfreithiol yn cael eu cychwyn gan drydydd parti yn eich erbyn a'ch bod wedi cydymffurfio â'r polisi hwn, gallwn gymryd camau i wneud yn hysbys bod eich gweithredoedd wedi'u cynnal yn unol â'r polisi hwn.