RFC 2350 – AM-CERT

Տարբերակ 1.1 - 2023-12-28

1.Տեղեկություն փաստաթղթի մասին

Սույն փաստաթուղթը ներկայացնում է AM-CERT-ի վերաբերյալ հիմնական տեղեկությունները, նկարագրում պարտականությունները և տրամադրվող ծառայությունները՝ համաձայն RFC 2350 ստանդարտի:

1.1. Վերջին թարմացման ամսաթիվ

Տարբերակ 1.1, հրապարակված 2023 թ. դեկտեմբերի 28-ին:

1.2. Ծանուցումներ թարմացումների մասին

AM-CERT-ը չի նախատեսում հաճախակի փոփոխություններ կատարել սույն փաստաթղթում, ուստի ընթացիկ տարբերակի հետ կարող եք ծանոթանալ 1.3 բաժնում: Փաստաթղթի թարմացումների և դրա վերաբերյալ հարցերի դեպքում կարող եք դիմել AM-CERT թիմին՝ cert@am-cert.am էլ. փոստով:

1.3. Փաստաթղթի գտնվելու վայրերը

Սույն փաստաթղթի ընթացիկ և թարմացված տարբերակը հասանելի է AM-CERT-ի կայքում՝ հետևյալ հղմամբ:

1.4. Փաստաթղթի իսկության հաստատումը

Սույն փաստաթուղթը ստորագրվել է AM-CERT-ի PGP բանալու միջոցով: Ստորագրությունը և մեր հանրային PGP բանալին (ID և մատնահետք) հասանելի են մեր կայքում և սույն փաստաթղթի 2.8 բաժնում:

1.5. Փաստաթղթի նույնականացում

Վերնագիր՝ AM-CERT_RFC2350_AM:

Տարբերակ՝ 1.1:

Փաստաթղթի կազմման ամսաթիվ՝ 2023 թ. դեկտեմբերի 28:

Վավերականության ժամկետ՝ փաստաթուղթը վավեր է մինչ հաջորդ թարմացման հրապարակումը:

2. Կոնտակտային տվյալներ

2.1. Թիմի անվանում

AM-CERT, Հայաստանի ազգային CERT (համակարգչային պատահարների արձագանքման թիմ) կամ CSIRT (համակարգչային անվտանգության միջադեպերի արձագանքման թիմ):

2.2. Հասցե

Վազգեն Սարգսյան փ. 26/1, 0010 Երևան, Հայաստանի Հանրապետություն:

2.3. Ժամային գոտի

Հայաստանի ժամանակով (AMT)՝ UTC/GMT + 4:

2.4. Հեռախոսահամար

+374 12 20 80 80

2.5. Ֆաքս

Կիրառելի չէ:

2.6. Հեռահաղորդակցության այլ ուղիներ

Հասանելի են ըստ անհրաժեշտության:

2.7. Էլեկտրոնային փոստի հասցե

Կիբեռանվտանգության միջադեպի կամ կիբեռսպառնալիքի վերաբերյալ հարցում իրականացնելու նպատակով անհրաժեշտ է կապվել AM-CERT-ի հետ cert@am-cert.am էլ. փոստով:

2.8. Հանրային բանալիներ և գաղտնագրման մասին տեղեկություն

PGP-ն օգտագործվում է AM-CERT-ի հետ տեղեկություն փոխանակելիս գաղտնիության և ամբողջականության ապահովման համար:

- Օգտատիրոջ նույնականացման համար (User ID) ՝ AM-CERT (National CERT/CSIRT Armenia) <cert@am-cert.am>
- Հավաստագրման հիմնական բանալու նույնականացման համար (Certify only master key ID) ՝ 0x03C1F5C8C45A21EF
- Հավաստագրման ենթաբանալու էլ. մատնահետք (Certify only master key fingerprint)՝ C6CE 4B08 9EB6 7D59 E2A5 D80F 03C1 F5C8 C45A 21EF

- Ստորագրման ենթաբանալու նույնականացման համար (Signing only sub key ID)՝ 0xC72C6282E210A114
- Ստորագրման ենթաբանալու էլ. մատնահետք (Signing only sub key fingerprint)՝ E8A8 D8D6 0CE2 88B6 4781 B9C9 C72C 6282 E210 A114
- Գաղտնագրման ենթաբանալու նույնականացման համար (Encryption only sub key ID)՝ 0x55B9DDDBC5E81FDE
- Գաղտնագրման ենթաբանալու էլ. մատնահետք (Encryption only sub key fingerprint)՝ 4BD0 1BFA E73C 371E 6EBB 4CF7 55B9 DDDB C5E8 1FDE

Հանրային PGP բանալին հասանելի է այստեղ, ինչպես նաև հայտնի հանրային բանալիների սերվերներում՝ https://pgp.circl.lu/ կամ https://pgp.mit.edu/.

2.9. Թիմի անդամներ

AM-CERT թիմի անդամ տեղեկատվական անվտանգության փորձագետների ցուցակը հրապարակման ենթակա չէ: AM-CERT թիմի անդամների ինքնությունը կարող է բացահայտվել միջադեպի շրջանակում՝ ըստ «անհրաժեշտ է իմանալ» (need-to-know) սկզբունքի։

2.10. Այլ տեղեկություններ

AM-CERT-ի վերաբերյալ տեղեկությունները հասանելի են պաշտոնական կայքում:

2.11. Հետադարձ կապ

Միջադեպերի վերաբերյալ հաղորդման նախընտրելի տարբերակն է կայքում հրապարակված առցանց ձևաթուղթը:

Միջադեպերի մասին հաղորդագրությունները կարող են ուղարկվել նաև սույն փաստաթղթում նշված էլ. հասցեով՝ օգտագործելով 2.8 բաժնում ներկայացված կրիպտոգրաֆիկ բանալին՝ տեղեկության ամբողջականությունն ու գաղտնիությունն ապահովելու նպատակով։

Արտակարգ իրավիճակների դեպքում անհրաժեշտ է էլ. նամակի թեմա դաշտում նշել [URGENT]։

AM-CERT-ը գործում է 24/7 ռեժիմով։

3. Կանոնադրություն

3.1. Առաքելություն

AM-CERT-ը Հայաստանի ազգային CERT-ն է (համակարգչային պատահարների արձագանքման թիմ) կամ CSIRT-ը (համակարգչային անվտանգության միջադեպերի արձագանքման թիմ)։ AM-CERT-ի առաքելությունն է ուսումնասիրել և համակարգել

կիբեռանվտանգության միջադեպերի արձագանքումը Հայաստանի ազգային կրիտիկական ենթակառուցվածքների համար:

AM-CERT-ի առաքելության շրջանակը ներառում է միջադեպերի կանխարգելումը, հայտնաբերումը, արձագանքը և հետմիջադեպային վերականգնումը, մասնավորապես՝

- Գործընկեր կազմակերպություններում ի հայտ եկած միջադեպերին առնչվող տեխնիկական աջակցության հայտերի արձագանքում,
- Կիբեռսպառնալիքների վերաբերյալ տեղեկության շրջանառում գործընկերների շրջանում,
- Կիբեռանվտանգության ոլորտում լավագույն փորձի կիրառման խթանում,
- Համագործակցություն կիբեռանվտանգության միջադեպերի արձագանքման միջազգայնորեն ճանաչված հաստատությունների և թիմերի հետ (CSIRTs, CERTs):

3.2. Գործընկերներ

AM-CERT-ի առաջնային գործընկերներն են Հայաստանի ազգային կրիտիկական ենթակառուցվածքի համակարգողները և ծառայություն մատուցողները՝ բացառությամբ պետական և ռազմական մարմինների: AM-CERT-ը նշված կազմակերպությունների համար հանդիսանում է կենտրոնական կոնտակտային մարմին և համակարգում է կիբեռանվտանգության միջադեպերի լուծմանն ուղղված աշխատանքները: Վերջինն իրականացվում է պատասխանատու մարմիններին արձագանքող և կանխարգելող ծառայություններ մատուցելու միջոցով:

Երկրորդային գործընկերներն են ՀՀ-ում գրանցված այն մասնավոր կազմակերպությունները, որոնք չեն մատուցում կրիտիկական ծառայություններ: Վեջիններ նույնպես կարող են օգտվել AM-CERT-ի ծառայություններից:

3.3. Պատկանելություն

AM-CERT-ը Հայաստանի տեղեկատվական համակարգերի գործակալության (ՀՏՀԳ) կիբեռանվտանգության բաժնի ստորաբաժանում է:

3.4. Լիազորություններ

AM-CERT-ի լիազորությունների սահմանումը նախատեսվում է Կիբեռանվտանգության մասին ՀՀ օրենքով, որը սույն փաստաթղթի հրապարակման պահին հանրային քննարկման փուլում է:

3.5. Հիմնադրում

Հայաստանի տեղեկատվական համակարգերի գործակալությունը և դրա շրջանակում գործող AM-CERT կենտրոնը հիմնադրվել են 2022թ ապրիլի 11-ին՝ համաձայն ՀՏՀԳ

կանոնադրության։ Թիմի
գործունեության սկիզբն է համարվում 2023թ սեպտեմբերի 1-ը

4. Քաղաքականություն

4.1. Միջադեպերի տեսակները և աջակցության մակարդակը

AM-CERT-ի կողմից տրամադրվող աջակցության շրջանակը կախված է միջադեպի տեսակից, լրջությունից, միջադեպի մասին հաղորդող գործընկերոջ գործունեության առանձնահատկություններից, կրիտիկական ենթակառուցվածքի կամ ծառայության վրա ազդեցության մակարդակից և տվյալ պահին AM-CERT-ի ռեսուրսներից:

AM-CERT-ը տրամարդում է հետևյալ արձագանքող և կանխարգելող ծառայությունները.

- 24/7 ռեժիմով հերթապահություն,
- Միջադեպերի վերլուծություն և փորձաքննություն,
- Միջադեպերի արձագանքման աջակցություն,
- Միջադեպերի արձագանքումը և դրանց հետևանքների վերացում (հեռավար և տեղային):
- Խոցելիությունների և վնասակար ծրագրերի վերլուծություն:

4.1.1. Համագործակցություն, ներգրավվածություն և տեղեկության բացահայտում

Միջադեպի հետ կապված տեղեկությունները, այդ թվում՝ ներգրավված անձանց անունները և միջադեպի տեխնիկական մանրամասները, չեն հրապարակվում առանց

ներգրավված շահառուների համաձայնության: AM-CERT-ը պարտավորվում է ապահովել միջադեպի վերաբերյալ տեղեկությունների գաղտնիությունը և դրանք չփոխանցել երրորդ անձանց, բացառությամբ օրենքով նախատեսված դեպքերի:

AM-CERT-ը կարող է գործընկեր կազմակերպություններից ստանալ կազմակերպության կամ արտադրանքի հետ կապված կասկածելի գործողությունների, միջադեպերի և խոցելիությունների մասին հաղորդումներ և մշակել ստացված տեղեկությունները:

AM-CERT-ի գործունեության շրջանակում տեղեկությունը փոխանցվում է ըստ դրա դասակարգման և ըստ «անհրաժեշտ է իմանալ» սկզբունքի:

Բոլոր այն դեպքերում, երբ AM-CERT-ին տրամադրված տեղեկությունը դասակարգված է ըստ Traffic Light Protocol (TLP)-ի, AM-CERT-ը հետևում է FIRST-ի կողմից սահմանված տեղեկության շրջանառման քաղաքականությանը:

4.2. Հաղորդակցություն և նույնականացում

AM-CERT-ի հետ հաղորդակցման ուղիները նկարագրված են սույն փաստաթղթի 2.11 բաժնում, իսկ նույնականացման նպատակով կիրառվող մեթոդները՝ 2.8 բաժնում:

5. Ծառայություններ

5.1. Միջադեպերի արձագանքում

AM-CERT-ի միջադեպերի արձագանքման ծառայությունները մեր գործընկերներին հասանելի են 24/7 ռեժիմով: Սույն բաժնում ներկայացված են AM-CERT-ի կողմից տրամադրվող միջադեպերի արձագանքման ծառայությունները:

5.1.1. Միջադեպերի դասակարգում՝ ըստ առաջնահերթության

- Միջադեպի լրջության գնահատում (արձագանքման առաջին մակարդակ),
- Միջադեպի մասշտաբի որոշում:

5.1.2. Միջադեպի համակարգում

- Միջադեպի հետ կապված տեղեկության դասակարգում (գրանցամատյաններ, կոնտակտային տվյալներ և այլն)՝ բացահայտման քաղաքականության համաձայն,
- Միջադեպի վերաբերյալ ծանուցում ներգրավված այլ գործընկերներին՝ «անհրաժեշտ է իմանալ» սկզբունքի համաձայն:

5.1.3. Միջադեպի լուծում

- Վարակված համակարգերի վերլուծություն

- Միջադեպերի լուծման գործընթացի շարունակում:

5.2. Կանխարգելիչ գործունեություն

- Կիբեռ միջավայրի ընդհանուր վերլուծություն,
- Տեղեկության շրջանառում, կիբեռսպառնալիքների, խոցելիությունների և հաղորդումների վերաբերյալ տեղեկության հրապարակում:

6. Միջադեպերի հաղորդման ձևաթղթեր

Ազգային կրիտիկական ենթակառուցվածքների օպերատորների կողմից կիբեռանվտանգության միջադեպերի մասին տեղեկության տրամադրման ուղիները նկարագրված են սույն փաստաթղթի 2.11 բաժնում:

7. Պատասխանատվություն

AM-CERT թիմը ձեռնարկում է բոլոր անհրաժեշտ քայլերը՝ տեղեկությունների, ծանուցումների և ահազանգերի պատրաստման ընթացքում անճշտությունները բացառելու նպատակով: Սակայն, AM-CERT-ը պատասխանատվություն չի կրում ստացվող և շրջանառվող տեղեկություններում առկա սխալների կամ բացթողումների, ինչպես նաև այդ տեղեկության օգտագործման հետևանքով առաջացած վնասների համար: