नेपाल सरकार
स्वास्थ्य तथा खाद्य स्वच्छता मन्त्रालय
सूचना प्रविधि तथा इ-हेल्थ शाखा
सिंहदरवार, काठमाडौं

मिति: २०८३/०७/१२

साइबर सुरक्षा सम्बन्धी अत्यन्त जरुरी सूचना
(PHP तथा Node.js Runtime मा देखिएका गम्भीर सुरक्षा कमजोरी तत्काल समाधान गर्ने सम्बन्धमा)

प्रधानमन्त्री तथा मन्त्रिपरिषद्को कार्यालय अन्तर्गतको राष्ट्रिय साइबर सुरक्षा केन्द्र, सिंहदरबारबाट मिति २०८३/०७/०५ मा PHP Runtime (Apache mod_php, PHP-FPM, php-cgi, FrankenPHP, LiteSpeed आदि) तथा यससँग सम्बन्धित Ecosystem (WordPress, Joomla, Drupal, Magento आदि) मा देखिएका दुई गम्भीर सुरक्षा कमजोरी (CVE-2026-109618 र CVE-2026-109619) सम्बन्धी "अत्यन्त जरुरी साइबर सुरक्षा एडभाइजरी" तथा मिति २०८३/०७/११ मा Node.js Runtime मा देखिएको Node2Shell (CVE-2026-111497) लगायतका कमजोरी सम्बन्धी साइबर सुरक्षा एडभाइजरी (Advisory Number: NCSC-1146-115-05) जारी भएका छन् । यी कमजोरीको दुरुपयोग भएमा सम्बन्धित प्रणालीमा अनधिकृत पहुँच प्राप्त हुने, सेवा अवरुद्ध हुने तथा प्रणालीमाथि अनधिकृत नियन्त्रण कायम हुन सक्ने जोखिम रहेको छ ।

स्वास्थ्य संस्थाहरूमा सञ्चालित अस्पताल व्यवस्थापन सूचना प्रणाली (HMIS), इलेक्ट्रोनिक स्वास्थ्य अभिलेख (EMR/EHR), बिलिङ, प्रयोगशाला, अनलाइन टिकट/अपोइन्टमेन्ट प्रणाली तथा वेबसाइट लगायतमा बिरामीको संवेदनशील व्यक्तिगत तथा स्वास्थ्य सम्बन्धी विवरण रहने हुँदा यी कमजोरीले स्वास्थ्य सेवा प्रवाह तथा बिरामीको गोपनीयतामा गम्भीर असर पार्न सक्ने देखिन्छ । तसर्थ, **यस मन्त्रालय मातहतका सम्पूर्ण विभाग, केन्द्र, अस्पताल तथा कार्यालयहरू एवं ती निकायका प्रणाली सञ्चालक तथा सेवा प्रदायक (Vendor) हरूले** देहायबमोजिमका कार्य तत्काल सम्पन्न गरी कार्यान्वयन प्रतिवेदन यस शाखामा पठाउनुहुन सम्बन्धित सबैको जानकारीका लागि यो सूचना प्रकाशित गरिएको छ ।

१. प्रणालीको पहिचान: आफ्नो निकायमा सञ्चालित सबै सर्भर, वेबसाइट तथा वेब एप्लिकेसनमा PHP वा Node.js प्रयोग भए/नभएको र प्रयोग भएको Version यकिन गर्नुहोस्। इन्टरनेटबाट पहुँच हुने (Internet-facing) प्रणालीलाई पहिलो प्राथमिकतामा राख्नुहोस्।

२. PHP अपग्रेड: PHP प्रयोग भएका प्रणालीलाई यथाशीघ्र देहायको Version वा सोभन्दा पछिको Version मा अपग्रेड गर्नुहोस्:

हालको Version	अपग्रेड गर्नुपर्ने न्यूनतम Version
PHP 8.5	8.5.12 वा सोभन्दा पछिको
PHP 8.4	8.4.27 वा सोभन्दा पछिको
PHP 8.3	8.3.36 वा सोभन्दा पछिको
PHP 8.2	8.2.35 वा सोभन्दा पछिको
PHP 8.1 वा सोभन्दा पुरानो	सुरक्षा Patch जारी नहुने भएकाले अनिवार्य रूपमा Support भइरहेको सुरक्षित नयाँ Version मा स्थानान्तरण गर्नुहोस्

३. Node.js अपग्रेड: Node.js प्रयोग भएका प्रणालीलाई देहायबमोजिम अपग्रेड गर्नुहोस्:

हालको Version	गर्नुपर्ने कार्य
Node.js 26.x (Current LTS)	26.12.1 वा सोभन्दा पछिको Version मा अपग्रेड
Node.js 24.x (LTS)	24.22.1 वा सोभन्दा पछिको Version मा अपग्रेड
Node.js 22.x (LTS)	22.23.4 वा सोभन्दा पछिको Version मा अपग्रेड (यसको End-of-Life April 30, 2027 रहेकाले Node.js 24 वा 26 LTS मा स्थानान्तरणको योजना बनाउनुहोस्)
Node.js 25.x, 23.x, 20.x, 18.x वा पुरानो (End-of-Life)	सुरक्षा Patch जारी नहुने भएकाले Compatibility परीक्षण गरी Node.js 24 LTS वा 26 LTS मा स्थानान्तरण गर्नुहोस्

४. सेवा पुनः सुरु (Restart/Redeploy): Disk मा Patch गरेर मात्र पुग्दैन । PHP का हकमा PHP-FPM, Apache तथा Queue Worker, Scheduler, Daemon लगायत लामो समय चल्ने सबै Process पुनः सुरु गर्नुहोस् ।Node.js का हकमा Application, Container तथा Serverless Function नयाँ Runtime बाट Rebuild/Redeploy गरी पुरानो वा Bundled Node.js Binary प्रयोगमा नरहेको सुनिश्चित गर्नुहोस् । Docker प्रयोग गर्ने प्रणालीमा Base Image अद्यावधिक गरी Image पुनः Build गर्नुहोस् ।

५. Patch नभएसम्म प्रणाली Online नगर्ने: Patch/अपग्रेड सम्पन्न भई परीक्षण नगरेसम्म प्रभावित Internet Facing प्रणालीलाई सार्वजनिक इन्टरनेटमा (Online) सञ्चालन नगर्नुहोस् । Patch सम्पन्न भएपछि मात्र प्रणाली पुनः Online गर्नुहोस् । बीचको अवधिमा आन्तरिक प्रयोग आवश्यक भएमा VPN, IP Allowlist वा Zero-Trust Gateway मार्फत मात्र पहुँच दिनुहोस् । End-of-Life Version भएका प्रणालीलाई छुट्टै Network मा

Isolate गरी बाहिर जाने (Egress) Traffic रोक्नुहोस् । WAF/Firewall Rule ले जोखिम केही घटाए पनि पूर्ण समाधान नहुने र अपग्रेड नै एकमात्र सुरक्षित विकल्प भएकाले यसलाई अस्थायी उपायका रूपमा मात्र लिनुहोस् । प्रणाली Offline रहेको अवधिमा बिरामी सेवा प्रवाहमा अवरोध नआउने गरी वैकल्पिक व्यवस्था मिलाउनुहोस् ।

६. तेस्रो पक्ष (Vendor) बाट सञ्चालित प्रणाली: सफ्टवेयर कम्पनी वा सेवा प्रदायकबाट विकास तथा सञ्चालन भएका प्रणालीको हकमा सम्झौताबमोजिम निजलाई तत्काल Patch गर्न लगाई अद्यावधिक Version सहितको लिखित पुष्टि लिनुहोस् ।

७. परीक्षण तथा निगरानी: अपग्रेडपछि प्रणालीले Patch गरिएको Version नै प्रयोग गरिरहेको, सेवा सामान्य रूपमा सञ्चालन भइरहेको र Log मा त्रुटि नदेखिएको सुनिश्चित गर्नुहोस् । सुरक्षा कमजोरीको दुरुपयोग भएको आशंका भएमा सम्बन्धित प्रणालीका Log तथा अन्य डिजिटल प्रमाण सुरक्षित राखी प्रणाली Isolate गर्नुहोस्, Password/API Key लगायतका Credential परिवर्तन गर्नुहोस् र तत्काल राष्ट्रिय साइबर सुरक्षा केन्द्र तथा यस शाखालाई जानकारी गराउनुहोस् ।

८. कार्यान्वयन प्रतिवेदन: Patch/अपग्रेड सम्पन्न भएपछि अनुसूची-१ बमोजिमको ढाँचामा यस शाखाको इमेल ठेगाना it.section@mohp.gov.np मा प्रतिवेदन पठाउनुहुन अनुरोध छ । आफ्नो निकायमा PHP वा Node.js प्रयोग नभएको अवस्थामा पनि सोही व्यहोरा खुलाई प्रतिवेदन पठाउनुहुन अनुरोध छ।

अनुसूची-१: कार्यान्वयन प्रतिवेदनको ढाँचा

निकायको नाम: .... सम्पर्क व्यक्ति तथा फोन: ....

क्र.सं.	प्रणाली/वेबसाइटको नाम	URL/IP ठेगाना	Runtime (PHP/Node.js)	साबिकको Version	अपग्रेड पछिको Version	Patch गरेको मिति	सञ्चालक (आफ्नै/Vendor)	कैफियत
१								
२								
३								

प्रमाणित गर्ने: .... पद: .... मिति: ....